

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE**

FINJAN SOFTWARE, LTD., an Israel  
corporation,

Plaintiff,

v.

SECURE COMPUTING CORPORATION,  
a Delaware corporation, CYBERGUARD,  
CORPORATION, a Delaware corporation,  
WEBWASHER AG, a German corporation  
and DOES 1 THROUGH 100,

Defendants.

C. A. No. 06-369-GMS

**APPENDIX OF EXHIBITS TO DECLARATION OF KRISTOPHER  
KASTENS IN SUPPORT OF PLAINTIFF FINJAN SOFTWARE, LTD.'S  
POST-TRIAL MOTION FOR INVALIDITY OF U.S. PATENT NO.  
7,185,361 PURSUANT TO FED. R. CIV. P. 50(b)**

**VOLUME 2 – EXHIBIT 3 (PARTS 2-6)**

OF COUNSEL:

Paul J. Andre  
Lisa Kobialka  
King & Spalding LLP  
1000 Bridge Parkway  
Redwood City, CA 94065  
(650) 590-0700

Philip A. Rovner (#3215)  
POTTER ANDERSON & CORROON LLP  
Hercules Plaza  
P. O. Box 951  
Wilmington, DE 19899  
(302) 984-6000  
[provner@potteranderson.com](mailto:provner@potteranderson.com)

Attorneys for Plaintiff  
Finjan Software, Ltd.

Dated: April 25, 2008

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE**

**CERTIFICATE OF SERVICE**

I, Philip A. Rovner, hereby certify that on April 25, 2008, the within document was filed with the Clerk of the Court using CM/ECF which will send notification of such filing(s) to the following; that the document was served on the following counsel as indicated; and that the document is available for viewing and downloading from CM/ECF.

**BY HAND DELIVERY AND E-MAIL**

Frederick L. Cottrell, III, Esq.  
Kelly E. Farnan, Esq.  
Richards, Layton & Finger, P.A.  
One Rodney Square  
920 N. King Street  
Wilmington, DE 19801  
[cottrell@rlf.com](mailto:cottrell@rlf.com); [farnan@rlf.com](mailto:farnan@rlf.com)

I hereby certify that on April 25, 2008 I have sent by E-mail the foregoing document to the following non-registered participants:

Jake M. Holdreith, Esq.  
Christopher A. Seidl, Esq.  
Robins, Kaplan, Miller & Ciresi L.L.P.  
2800 LaSalle Plaza  
800 LaSalle Avenue  
Minneapolis, MN 55402  
[jmholdreith@rkmc.com](mailto:jmholdreith@rkmc.com) ; [caseidl@rkmc.com](mailto:caseidl@rkmc.com)

/s/ Philip A. Rovner  
Philip A. Rovner (#3215)  
Potter Anderson & Corroon LLP  
Hercules Plaza  
P.O. Box 951  
Wilmington, Delaware 19899  
(302) 984-6000  
E-mail: [provner@potteranderson.com](mailto:provner@potteranderson.com)

# **EXHIBIT 3**

## **PART 2**

## Session Authentication — Deployment

The file is in the standard .INI format. It is divided into sections, each of which consists of a list of parameters and their values (FIGURE 1-29).

```
[FireWall]
IPAddress=
Any=FALSE
[Cache]
Method=Every time
Timeout=30
```

FIGURE 1-29 SETUP.INI file

The Session Authentication agent for Windows included with FireWall-1 provides for password caching and for restricting authentication to specific FireWalls.

When you start the Session Authentication agent, it is minimized and its icon appears in the system tray. From this point on, one of two things can happen:

- The user can open the Session Authentication agent and configure it.
- The Session Authentication agent can receive an authentication request from a FireWall Module.

#### Session Authentication Rule Properties

To display the **Session Authentication Action Properties** window (FIGURE 1-30) for a Session Authentication rule, double-click on the rule's **Action**.

In the **Session Authentication Action Properties** window, specify parameters that define Session Authentication for the rule.

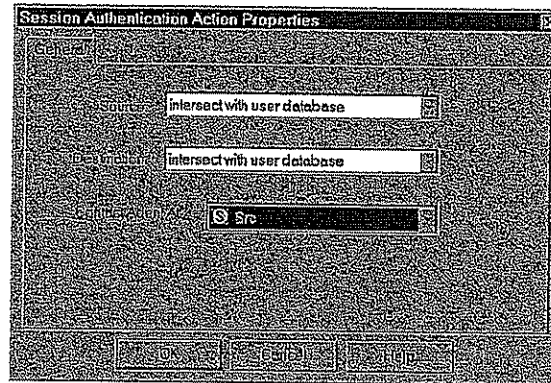


FIGURE 1-30 Rule Authentication Properties window for a Session Authentication Rule



## Session Authentication

**Source** — Reconcile **Source** in the rule with **Allowed Sources** in the **User Properties** window.

The **Allowed Sources** field in the **User Properties** window may specify that the user to whom this rule is being applied is not allowed access from the source address, while the rule may allow access. This field indicates how to resolve this conflict.

- Choose **Intersect with User Database** to apply the intersection of the access privileges specified in the rule and in the **User Properties** window.
- Choose **Ignore User Database** to allow access according to the **Source** specified in the rule.

See "Example" on page 39 for further information.

**Destination** — Reconcile **Destination** in the rule with **Allowed Destinations** in the **User Properties** window.

The **Allowed Destinations** field in the **User Properties** window may specify that the user to whom this rule is being applied is not allowed access to the destination address, while the rule may allow access. This field indicates how to resolve this conflict.

- Choose **Intersect with User Database** to apply the intersection of the access privileges specified in the rule and in the **User Properties** window.
- Choose **Ignore User Database** to allow access according to the **Destination** specified in the rule.

See "Example" on page 39 for further information.

**Contact Agent At** — Select the computer on which the Session Authentication Agent for this rule is running.

- Choose **Src** to specify that the Session Authentication Agent on the session's **Source** object will authenticate the session.

This is the most commonly used option.

- Choose **Dst** to specify that the Session Authentication Agent on the session's **Destination** object will authenticate the session.

This option would normally be used for the X protocol.

- Choose one of the computers in the list to specify that the Session Authentication Agent that will authenticate this session is running on that computer. The computers displayed in the list are the network objects defined as machines (both internal and external).

This option enables an administrator to manually authorize connections.

## Session Authentication — Deployment

## Logging and Tracking

Logging and tracking is specified in two places for Session Authentication:

- **Authentication Failure Track** in the **Authentication** tab of the **Properties Setup** window (FIGURE 1-9 on page 36)

The options under **Authentication Failure Track** specify the action to take for failed authentication. These options apply to all rules.

- **Rule Base Track**

The tracking for a successful Authentication attempt is determined by the **Track** field of the applied Session Authentication rule.

## How the User Authenticates

When a local user in the rule depicted in FIGURE 1-25 on page 68 initiates a connection to the Internet, the FireWall Module on the gateway intercepts the connection and requests that the Session Authentication agent authenticate a user. The Session Authentication agent displays the **Session Authentication** window (FIGURE 1-31).

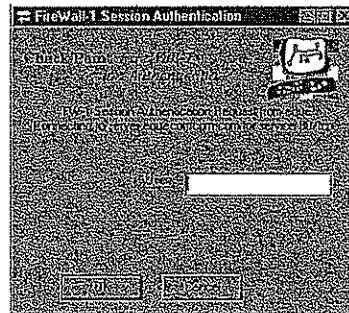
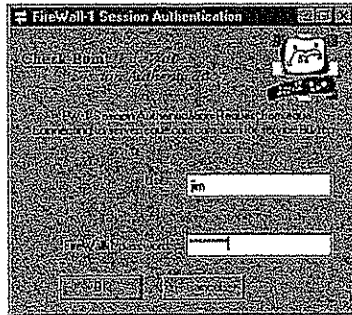


FIGURE 1-31 Session Authentication window — user prompt

### Session Authentication

The user enters his or her user name, and is then prompted to enter a password (FIGURE 1-32).



**FIGURE 1-32** Session Authentication window — password prompt

The form of the password prompt depends on the user's Authentication method.

Overview

## Client Authentication

### In This Section

Overview	page 75
Client Authentication — Deployment	page 78
How the User Initiates Client Authentication	page 87
Security Considerations — Client Authentication	page 96
Client Authentication — Additional Features	page 96

### Overview

Client Authentication allows connections from a specific IP address after successful authentication. In contrast to User Authentication, which allows access per user, Client Authentication allows access per IP address. The user working on a client performs the authentication by providing a name and password, but it is the client that is granted access.

Client Authentication is less secure than User Authentication because it allows multiple users and connections from the authorized IP address or host. The authorization is per machine, because the supported services do not have an initial login procedure. For example, if FINGER is authorized for a client machine, then all users on the client are authorized to use FINGER, and will not be asked to supply a password during the authorization period. For this reason, Client Authentication is best enabled for single user machines.

The advantage of Client Authentication is that it can be used for any number of connections, for any service and the authentication is valid for any length of time.

Consider the following rules:

No.	Source	Destination	Service	Action	Track	Install On
1	Sales@Tower	DBaseHost	Lotus	Client Auth	Long	Gateways
2						
3						

FIGURE 1-33 Example Client Authentication Rule Base

In the example rules shown in FIGURE 1-16, the first rule specifies Client Authentication for lotus service connections whose destination is a database server. The **Source** of a Client Authentication rule indicates the group of users that can

## Client Authentication

authenticate, and the host or hosts from which they can authenticate. A user is authenticated according to the scheme defined in the **Authentication** tab of his or her **User Properties** window.

Unauthorized attempts to use the Lotus service on the database host will be detected by the second rule, and an alert will be issued.

Administrators can also define authorization periods and the number of permitted sessions. For example, a user working on Tower can sign on and authenticate at the start of the day and remotely access the database host throughout the day. At the end of the day, the user would sign off and close the connection with the database host.

## Initiating Client Authentication

### Sign On Methods

Sign On Methods specify how a user begins a Client Authentication session. Sign On Methods are specified in the **Client Authentication Action Properties** window of a rule. There are three Sign On methods:

#### ■ Manual Sign On

The Manual Sign On method requires a user to initiate the Client Authentication session on the gateway. Manual Sign On is not transparent, because the user must first connect to the gateway. The user may initiate the Client Authentication session in one of the following ways:

- TELNET session — the user starts a TELNET session on port 259 of the gateway
- Web Browser — the user requesting an HTTP connection to port 900 on the gateway using a Web browser.

FireWall-1 also supports encrypted Client Authentication through a Web browser. This feature is available for HTTPS (HTTP encrypted by SSL) only. The user can request an HTTPS connection to a specific port on the gateway. For more information on configuring the gateway to support HTTPS, see "Encrypted Client Authentication" on page 94.

#### ■ Partially Automatic Sign On

Partially Automatic Sign On provides transparent Client Authentication for authenticated services: HTTP, TELNET, RLOGIN, and FTP. A user working with one of these services can directly request the target host. The user is then prompted and signed on through the User Authentication mechanism. If authentication is successful, access is granted from the IP address from which the user initiated the connection.

This method is transparent because the user does not have to initiate a connection on the gateway before connecting to the target host. The disadvantage of using this method is that it is available only for authenticated services.

For an example using Partially Automatic Sign On, see "Partially Automatic Sign On Method" on page 92.

## Initiating Client Authentication

## ■ Fully Automatic Sign On

Fully Automatic Sign On provides transparent Client Authentication for all services. A user working with any service directly requests the target server. Users of authenticated services are signed on through the User Authentication mechanism, while users working with all other services are signed-on using the FireWall-1 Session Authentication Agent. If authentication is successful, access is granted from the IP address that initiated the connection.

Fully Automatic Sign On is transparent because the user does not have to initiate a Client Authentication session on the gateway before connecting to the target host. It is available for all services, but requires a FireWall-1 Session Authentication Agent on the client (in order to handle non-authenticated services).

It is recommended to use Fully Automatic Sign On only if you know users have the Session Authentication Agent installed on their machines. If users do not have the Session Authentication Agent, it is recommended to use the Partially Automatic sign on method. This at least allows users of authenticated services to open a Client Authentication session on the target host without having to connect to the gateway first.

For an example using Fully Automatic Sign On, see "Fully Automatic Sign On Method" on page 93.

For more information on the Firewall-1 Session Authentication Agent, see "Session Authentication" on page 66.

Partially and Fully Automatic Client Authentication rules allow users if they authenticate successfully, but do not necessarily reject the connection if the user fails authentication. In addition, the fact that a user successfully authenticates does not necessarily mean that there is a rule that allows that user access. This is because if the service is an authenticated service, the appropriate Security Server is invoked. The authenticating Security Server first checks if the connection can be allowed by a rule which does not require authentication. For more information, see "The 'Insufficient Information' Problem" on page 104 of Chapter 2, "Security Servers."

## How Services are Authorized

After successful authentication, the user can work with the services and hosts permitted by the rule, depending on the rule's authorization parameters. The **General** tab of the rule's **Client Authentication Action Properties** window specifies how the user works with the services permitted by the rule. For example, a user may be authorized to work with all the services and hosts permitted by the rule, or may have to request each service and host individually. For more information, see "Client Authentication Rule Properties" on page 81.



## Client Authentication

## Timeouts

Timeout periods and the number of sessions permitted are specified in the **Limits** tab of the **Client Authentication Action Properties** window. For more information, see "Client Authentication Action Properties Window — Limits Tab" on page 84.

## Client Authentication — Deployment

FIGURE 1-34 depicts a configuration in which a FireWalled gateway (London) protects a PC network (localnet) and a DMZ network, which includes a database server on the host Palace.

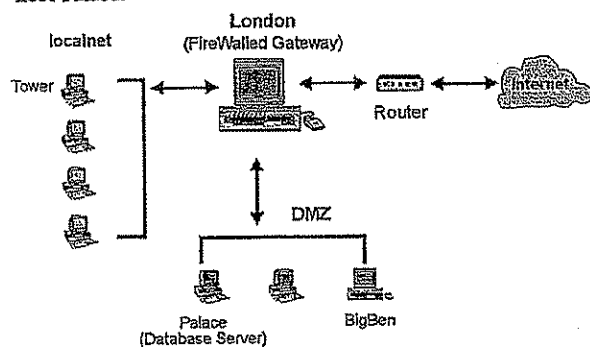


FIGURE 1-34 Example configuration — Client Authentication

A group of users in the QA department requires frequent access to the database on Palace. Access to Palace is allowed from localnet hosts. Each user can sign on at the beginning of the day and can use the service for a specified time period and number of sessions. If a user forgets to sign off, the connection to Palace is timed out at end of authorization period.

Access to the database server from QA users on Tower is enabled by the following rule:

No.	Source	Destination	Service	Action	Track	Install On
1	QA@Local_Net	Palace	Lotus	Client Auth	Long	Gateway

FIGURE 1-35 Example Client Authentication rule

To implement Client Authentication for this configuration, the administrator must define the following:

- the users who must authenticate before accessing the target server
- the gateway's supported authentication schemes
- Client Authentication rule properties

## Initiating Client Authentication

- Client Authentication properties that apply to all rules (i.e., tracking for unsuccessful authentication)
- logging and tracking

## Defining Client Authentication

## Users

In a Client Authentication rule, the **Source** must be a user group. You must first define the properties of the permitted users, such as their authentication schemes and the network objects from which they are allowed access. These properties are defined in the tabs of the **User Properties** window.

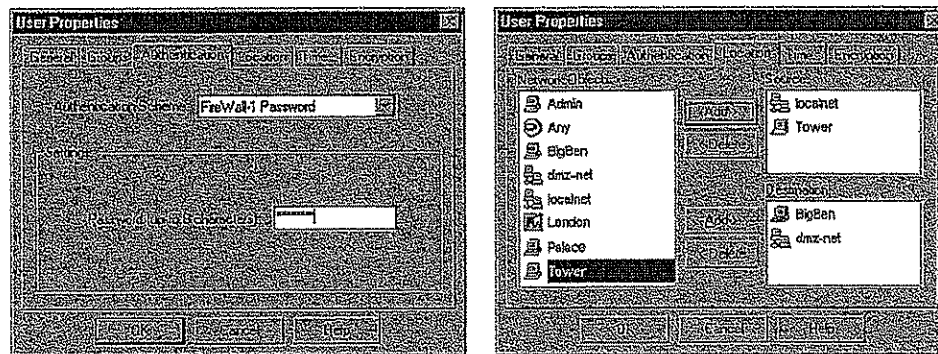


FIGURE 1-36 User Properties window - Authentication tab and Location tab

You must then define a group which includes the users who must authenticate before they access the database server.

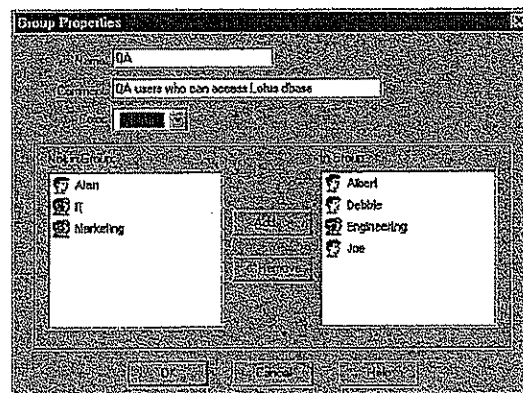


FIGURE 1-37 Group Properties window — Defining Permitted Users



## Client Authentication

For more information on defining users and user groups, see Chapter 3, "User Management" of *Managing FireWall-1 Using the Windows GUI* or *Managing FireWall-1 Using the OpenLook GUI*.

## User Access

The **Source** field also specifies the host or network object from which the user group is allowed access.

You can add a user group to a rule using the **User Access** window. To display the **User Access** window, right-click on the rule's **Source**, and choose **Add User Access** from the drop-down menu.

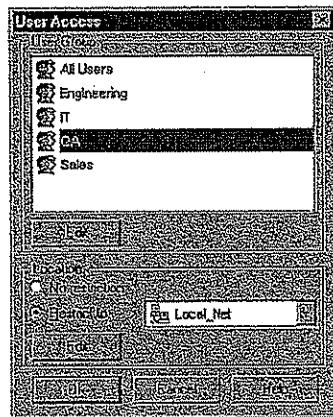


FIGURE 1-38 User Access window

Click on the user group you want to add.

The options under **Location** allow you to specify the objects from which the users in the selected group are allowed access.

If you choose **No Restriction**, then the users will be allowed access from any source.

If you choose **Restrict To**, you must then select the network object from which the users will be allowed access.

In the example depicted in FIGURE 1-38, users in the **QA** group will be allowed access only from the **Local\_Net** hosts.

## Initiating Client Authentication

## Supported Authentication Schemes

You must make sure the gateway supports the same authentication schemes you defined for your users. Gateway authentication schemes are defined in the **Authentication** tab of the gateway object's **Workstation Properties** window.

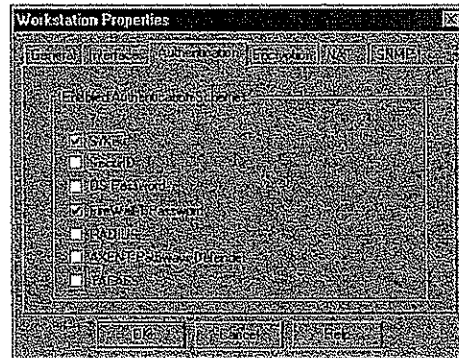


FIGURE 1-39 Workstation Properties window — Authentication tab

## Client Authentication Rule Properties

Rule Properties are defined in the tabs of the **Client Authentication Action Properties** window. Rule Properties include the following:

- how services are authorized
- authorization timeout periods
- the number of sessions allowed
- tracking for successful authentication

## Client Authentication Action Properties Window — General Tab

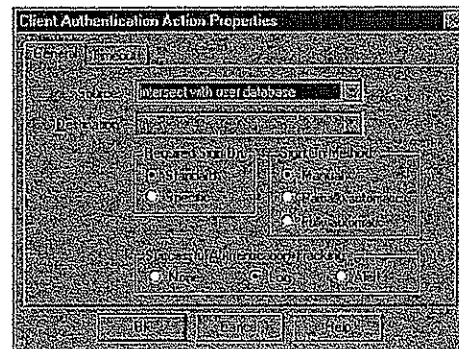


FIGURE 1-40 Client Authentication Action Properties window — General tab

## Client Authentication

The **General** tab specifies how to resolve the allowed sources and destinations defined in the **Location** tab of a user's **Properties** window with the **Source** and **Destination** allowed by the rule.

**Source** — Reconcile **Source** in the rule with **Allowed Sources** in **User Properties** window.

- Choose **Intersect with User Database** to apply the intersection of the access privileges specified in the rule and in the **User Properties** window.
- Choose **Ignore User Database** to allow access according to the **Source** specified in the rule.

For the configuration depicted in FIGURE 1-34 on page 78, if the **Location** tab of a **QA** user allowed access only from **Thames** on localnet, you would choose **Ignore User Database** to allow that user access from **Tower**, the allowed **Source** in the rule.

**Destination** — Reconcile **Destination** in the rule with **Allowed Destinations** in the **User Properties** window.

- Choose **Intersect with User Database** to apply the intersection of the access privileges specified in the rule and in the **User Properties** window.
- Choose **Ignore User Database** to allow access according to the **Destination** specified in the rule.



**Note** — If **Standard Sign-on** is specified in **Rule Requires** then this option is automatically set to **Ignore User Database** (because under **Standard Sign On**, the user can access all the destinations allowed by the rule). You can change this setting only if you specify **Specific Sign-on**. (See FIGURE 1-40 on page 81)

The following options in the **General** tab specify additional rule parameters.

#### How Services are Authorized

**Required Sign On** — These options specify how the services permitted by the rule are authorized. Select one of the following values:

- **Standard Sign-on** — All the services allowed for the user are authorized together. For an example of how **Standard Sign-on** is used, see "Example — **Standard Sign-on**" on page 89.
- **Specific Sign-on** — The user must request each service and destination individually. For example, if a rule specifies more than one service, then each service must be authorized separately. For an example of how **Specific Sign-on** is used, see "Example — **Specific Sign-on**" on page 90.

## Initiating Client Authentication

## How Client Authentication is Initiated

**Sign On Method** — Select one of the following values:

- **Manual** — The user must initiate Client Authentication on the gateway through either a TELNET session on port 259 or an HTTP session on port 900.

For an example using Manual Sign On with TELNET, see "Manual Sign On Using TELNET" on page 87.

For an example using Manual Sign On through a Web browser (HTTP), see "Manual Sign On — HTTP" on page 91.

- **Partially Automatic** — If a connection matches the rule, and the service is an authenticated service (RLOGIN, TELNET, HTTP, FTP), the user is signed on through User Authentication.

For an example using Partially Automatic Sign On, see "Partially Automatic Sign On Method" on page 92.

- **Fully Automatic** — If a connection using a non-authenticated service matches the rule, and the FireWall-1 Session Authentication Agent is installed on the client, the user is signed on by the Session Authentication Agent. If a connection using an authenticated service matches the rule, then the user is signed on through User Authentication.

For an example using Fully Automatic Sign On, see "Fully Automatic Sign On Method" on page 93.

## Tracking

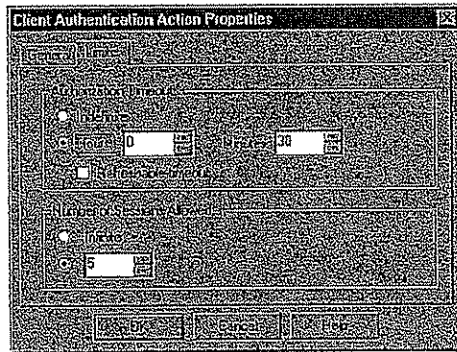
**Successful Authentication Tracking** — logging option for the sign-on session. Choose one of the following:

- **None** — no tracking
- **Log** — Long Log
- **Alert** — the Authentication Alert Command in the Log and Alert tab of the Properties Setup window

These settings specify logging and tracking for only the sign-on session. For information on additional logging and tracking parameters for Client Authentication, see "Logging and Tracking" on page 86.

## Client Authentication

Client Authentication Action Properties Window — Limits Tab

**FIGURE 1-41** Client Authentication Action Properties window — Limits tab

The **Limits** tab specifies the period during which the user is authorized to work with permitted services, and how many sessions are allowed.

**Authorization Timeout** — Specifies the length of time after the client is authenticated during which the user (at the source IP address specified under **Source** in the relevant rule in the Rule Base) may start the specified service.

Once the service is started, there is no restriction on how long it can remain open.

If you do not wish to restrict the authorization timeout period, check **Indefinite**.

**Refreshable Timeout** — the **Authorization Timeout** period is reset with every new connection authorized by the rule.

This option is useful if the user remains at the authorized client after successful authentication. For example, suppose that the **Authorization Timeout** is set to 15 minutes, **Refreshable Timeout** is checked, and the service allowed by the rule is **FINGER**. Then, a user who initiates a **FINGER** connection after 10 minutes resets the authorization period to 15 minutes.

If **Refreshable Timeout** is not checked, and the user does not start a **FINGER** connection during the 15-minute authorization timeout period, the session times out and the user must reauthenticate.

**Sessions Allowed** — the number of sessions (connections) allowed after the authentication

If you do not wish to restrict the number of sessions, check **Infinite**.



## Initiating Client Authentication

If the rule specifies a service group, and **Sessions Allowed** is not set to **Infinite**, then the number of sessions allowed for the services in the group depends on what is specified under **Required Sign On** in the **General** tab of the **Client Authentication Action Properties** window:

- If **Specific Sign On** is used, then each service in the group will be allowed the number of sessions specified. For example, if **Sessions Allowed** is set to **2**, and the service group consists of **FINGER** and **RSTAT**, then each service will be allowed two sessions.
- If **Standard Sign On** is used, then the number of sessions applies to all the services in the group together.

## Client Authentication Properties — Rule Base

The **Authentication** tab of the **Properties Setup** window specifies Client Authentication parameters that apply to all rules.

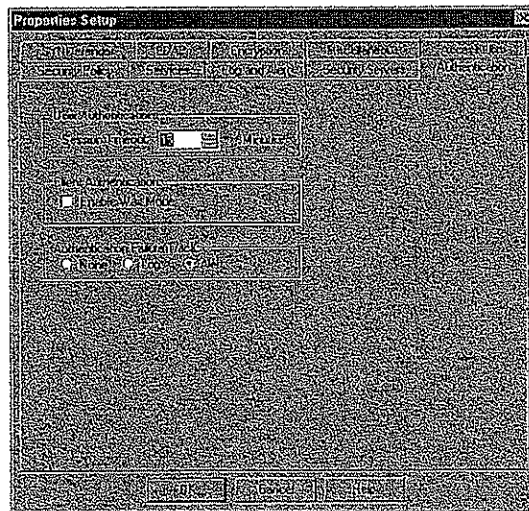


FIGURE 1-42 Properties Setup window — Authentication tab

**Enable Wait Mode** — This option applies only when the user initiates Client Authentication through a TELNET session to port 259 on the gateway. For information on using TELNET to initiate Client Authentication, see "Manual Sign On Using TELNET" on page 87.

If **Enable Wait Mode** is checked, the initial TELNET session remains open. The Client Authentication session is closed when the TELNET session is closed or timed out. Firewall-1 regularly pings the client during the authorization period. If

## Client Authentication

for some reason the client machine has suddenly stopped running (for example, because of a power failure), FireWall-1 closes the TELNET session and Client Authentication privileges from this IP address are withdrawn.



**Note – Enable Wait Mode** works only with Client Authentication rules which specify **Standard Sign On**. If you select **Enable Wait Mode**, Client Authentication rules which require **Specific Sign On** are not applied.

If **Enable Wait Mode** is not checked, the initial TELNET session is automatically closed when the user chooses **Standard Sign On** or **Specific Sign On**. The user must initiate another TELNET session to the gateway in order to sign off the Client Authentication session.

**Authentication Failure Track** — these options specify tracking for unsuccessful authentication attempts. These tracking options apply to all rules.

### Logging and Tracking

There are three places in which logging and tracking for Client Authentication is specified:

**1 Rule Base Editor — Track**

The tracking in this window applies to the initial communication attempt to the gateway for the authentication, and to the authenticated session.

**2 Authentication tab of the Properties Setup window — Authentication Failure Track (FIGURE 1-42 on page 85)**

The tracking in this window applies to all authentication failures.

**3 The General tab of the Client Authentication Action Properties window — Successful Authentication Track (FIGURE 1-40 on page 81)**

The tracking in this window applies to successful authentications.

For example, suppose that a Manual Sign On rule specifies **Client Authentication** for the user group **QA@Tower**. A QA user logs in to the gateway and attempts to initiate a TELNET session under the rule.

The tracking for the login attempt to the gateway is determined by the entry in the Rule Base **Track** for that rule.

If the user is successfully authenticated, then the tracking for the successful authentication attempt is determined by the entry in the rule's **Client Authentication Action Properties** window.

If the user fails the authentication, the tracking is determined by the entry in the **Authentication** tab of the **Properties Setup** window.

## Initiating Client Authentication

## Example

Source	Destination	Service	Action	Track	Install On
QAGLocal_Net	Palace	finger	Client Auth	Short	Gateways

Suppose a user wishes to start a Client Authentication session for the FINGER service on the host palace. The target host is behind the gateway London. The **Manual Sign On** method is specified in the **General** tab of the rule's **Client Authentication Action Properties** window.

First, the user attempts to TELNET to the gateway (London) by typing:

```
telnet london 259
```

The logging in effect for this step is defined in the **Track** column of the rule in the Rule Base that controls this user's ability to access TCP port 259 on london.

Next, the user is asked to specify the user name, password, and optionally host name and service.

If the user is successfully authenticated, then the tracking for the successful authentication attempt is determined by the entry in the **General** tab of the rule's **Client Authentication Action Properties** window. The user then starts a FINGER session on the target server. The tracking for the FINGER session is determined by the **Track** column of the above rule.

If the user fails the authentication, the tracking is determined by the entry in the **Authentication** tab of the **Properties Setup** window.

## How the User Initiates Client Authentication

## Manual Sign On Using TELNET

The rule depicted in FIGURE 1-43 allows Engineering users on a single host, Tower, access to the hosts Palace or Thames after successful Client Authentication. Palace protected by London, a FireWalled gateway.

Source	Destination	Service	Action	Track	Install On
Engineering@Tower	Palace Thames	rsh finger	Client Auth	Long	Gateways

FIGURE 1-43 Client Authentication Rule



## Client Authentication

An Engineering user wishing to access the destination hosts must first TELNET to London, the gateway:

```
telnet london 259
```

The user is then prompted for the following data:

- user name
- password

Next, the user is asked to choose:

```
Choose:
(1) Standard Sign-on
(2) Sign-off
(3) Specific Sign-on
```

If there is at least one matching rule that specifies **Standard Sign-on** in the **Rule Requires** field of the **Rule Client Authentication Properties** window (FIGURE 1-40 on page 81), then the user can choose **Standard Sign-on** from this menu. Otherwise, the user may choose only **Specific Sign-on** or **Sign-off**.

If the user chooses **Standard Sign-on**, then the authentication is for all services on all destination hosts, as allowed by the relevant rule or rules. The number of relevant rules is displayed by the Security Server if the authentication is successful (see FIGURE 1-44 on page 89).

If the user chooses **Specific Sign-on**, then the user is prompted for the service name and host name (FIGURE 1-45 on page 90).

If the user chooses **Sign-off**, then all permissions accorded to this IP address (the host from which the user initiated the session) are withdrawn, and the session is terminated (see FIGURE 1-46 on page 91).



**Note** - When Client Authentication is defined, FireWall-1 adds an implicit rule allowing TELNET connections to the authorization port (default 259) on the gateway. It is not necessary for the system administrator to explicitly add such a rule to the Rule Base. At the same time, the system administrator should not block access by another rule.

Once this data has been entered, the user receives either an "authorized" or "unauthorized" message, and the TELNET session is automatically closed (if **Enable Wait Mode** is not checked in the **Authentication** tab of the **Properties Setup** window).

If **Enable Wait Mode** is checked in the **Authentication** tab of the **Properties Setup** window, the TELNET session remains open. Client Authentication privileges are withdrawn from this IP address only when the TELNET session is closed or timed out.

## Initiating Client Authentication

Timeout periods and sessions allowed depend on what is specified in the **Limits** tab of the rule's **Client Authentication Action Properties** window.

If the user is authorized, the client machine is allowed to use the service on the specified host for the period specified in **Authorization Timeout**, unless the user signs off earlier.

The number of connections (sessions) allowed in the given time frame is determined by the **Sessions Allowed** parameter.

Example — Standard Sign-on

```
tower 1% telnet london 259
Trying 191.23.45.67 ...
Connected to london.
Escape character is '^]'.
CheckPoint FireWall-1 Client Authentication Server running on
london
Login: jim
FireWall-1 Password: *****
User authenticated by FireWall-1 auth.

Choose:
  (1) Standard Sign-on
  (2) Sign-off
  (3) Specific Sign-on

Enter your choice: 1

User authorized for standard services (1 rules)
Connection closed by foreign host.
```

**FIGURE 1-44** Client Authentication - Standard Sign-On for all Services and Destinations Allowed Under Rule

## Client Authentication

## Example — Specific Sign-on

```
tower 3% telnet london 259
Trying 191.23.45.67 ...
Connected to london.
Escape character is '^]'.
CheckPoint FireWall-1 Client Authentication Server running on
london
Login: jim
FireWall-1 Password: *****
User authenticated by Internal auth.

Choose:
  (1) Standard Sign-on
  (2) Sign-off
  (3) Specific Sign-on

Enter your choice: 3
Service: rstat
Host: palace
Client Authorized for service
Another one (Y/N): Y
Service: finger
Host: thames
Client Authorized for service
Another one (Y/N): n
Connection closed by foreign host.
```

FIGURE 1-45 Client Authentication - Specific Sign-On for two Services (Each One on a Different Host)

## Initiating Client Authentication

## Example — Sign-off

```

tower 2% telnet london 259
Trying 191.23.45.67 ...
Connected to London.
Escape character is '^]'.
CheckPoint FireWall-1 Client Authentication Server running on
London
Login: jim
FireWall-1 Password: *****
User authenticated by Internal auth.

Choose:
  (1) Standard Sign-on
  (2) Sign-off
  (3) Specific Sign-on

Enter your choice: 2

User was signed off from all services
Connection closed by foreign host.

```

FIGURE 1-46 Client Authentication - Signing Off

## Manual Sign On — HTTP

A user can initiate a Client Authenticated session by beginning an HTTP session on port 900 on the gateway. The requested URL must specify the gateway name and port as follows:



The browser prompts the user for a name and password. The browser then presents HTML pages listing the Client Authentication options described in "Manual Sign On Using TELNET" on page 87.



**Note** – When Client Authentication is defined, FireWall-1 adds an implicit rule allowing HTTP connections to the authorization port (default 900) on the gateway. It is not necessary for the system administrator to explicitly add such a rule to the Rule Base. At the same time, the system administrator should not block access by another rule.

## Client Authentication

## Partially Automatic Sign On Method

Partially Automatic Sign On provides transparent Client Authentication for authenticated services: HTTP, TELNET, RLOGIN, and FTP. A user working with one of these services directly requests the target host. If a connection using one of these services matches a partially automatic Client Authentication rule, the user is prompted and signed on through the User Authentication mechanism. If authentication is successful, access is granted from the IP address from which the user initiated the connection.

Suppose the following rule specifies **Partially Automatic Sign On** in the rule's **Client Authentication Action Properties** window (FIGURE 1-40 on page 81).

Source	Destination	Services	Action	Track	Install On
Sales@Tower	BigBen	ftp	ClientAuth	Long Log	Gateways

According to the above rule Jim, a Sales user at the host Tower can FTP directly to BigBen. The user on Tower is authenticated by the FireWall-1 FTP Security Server on the London, the gateway.

```
tower # ftp bigben
Connected to london.
220 london CheckPoint FireWall-1 secure ftp server running on
London
Name (bigben:jim): jimb
331-aftpd: FireWall-1 password: you can use use password@FW-1-
password
Password: <Unix password on bigben>@<FireWall-1 password>
230-aftpd: User jimb authenticated by FireWall-1 authentication.
230-aftpd: Connected to bigben. Logging in...
230-aftpd: 220 bigben ftp server (UNIX(r) System V Release 4.0)
ready.
230-aftpd: 331 Password required for jimb.
230 User jimb logged in.
```



**Note** – Although the user is authenticated by the Security Server, the connection is entered as a Client Authentication connection in the FireWall-1 connections table, and access is authorized from the IP address from which the user initiated the connection.

## Initiating Client Authentication

## Authorized Services

If **Standard Sign-On** is specified in the rule's **Client Authentication Action Properties** window, the user on the client machine is allowed to use all the services permitted by the rule for the authorization period without having to perform authentication for each service.

If **Specific Sign On** is specified, only connections which match the original connection are allowed without additional authentication. If a rule specifies more than one service or host, the user on the client must reauthenticate for each service or host. **Specific Sign On** is useful if you want to limit access to services and target hosts.

The authorization period and the number of connections (sessions) allowed are specified in the **Limits** tab of the rule's **Client Authentication Action Properties** window.

Consider the following Partially Automatic Sign On rule:

Source	Destination	Services	Action	Track	Install On
Sales@Tower	BigBen	ftp rlogin	ClientAuth	Long Log	Gateways

Suppose a user on Tower initiates an FTP session on BigBen and is successfully authenticated. The user can now work with FTP on BigBen for the specified authorization period without having to reauthenticate for each FTP connection. If the user on Tower closes the initial FTP session, and decides to initiate a new FTP session (within the authorized time period) to download additional files, he or she does not have to reauthenticate.

If the same user initiates an RLOGIN session to BigBen, he or she will have to reauthenticate if **Specific Sign On** is required. If **Standard Sign On** is required, then the user will not have to reauthenticate in order to use RLOGIN.

## Fully Automatic Sign On Method

Suppose the following rule specifies **Fully Automatic Sign On** in the rule's **Client Authentication Action Properties** window (FIGURE 1-40 on page 81).

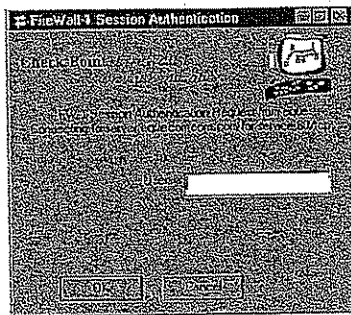
Source	Destination	Services	Action	Track	Install On
Sales@Tower	BigBen	any	ClientAuth	Long Log	Gateways

## Client Authentication

A user on Tower who initiates a connection to BigBen using any authenticated service is signed on through User Authentication. A user on Tower working with any other service, such as FINGER, is signed on through the FireWall-1 Session Authentication Agent (FIGURE 1-47).



**Note** – To enable Fully Automatic sign-on for non-authenticated services, the FireWall-1 Session Authentication Agent must be installed on the client.



**FIGURE 1-47** FireWall-1 Session Authentication Agent prompt

The user can work with services and destinations in the rule according to what is specified under **Required Sign On** in the **General** tab of the rule's **Client Authentication Action Properties** window (FIGURE 1-40 on page 81).

If **Standard Sign On** is specified, then the user can work with the all the services and destinations permitted by the rule without having to reauthenticate.

If **Specific Sign On** is specified, only connections which match the connection which opened the rule do not have to be reauthenticated.

The authorization period and the number of connections (sessions) allowed are specified in the **Limits** tab of the rule's **Client Authentication Action Properties** window.

## Encrypted Client Authentication

### HTTPS Connections

FireWall-1 Client Authentication also supports HTTPS (HTTP encrypted by SSL) connections. This feature is supported only for Client Authentication sessions initiated through a Web browser. To enable encrypted Client Authentication, the Administrator must modify the gateway and Security Server configuration file.



## Initiating Client Authentication

## Generating CA Keys

The Administrator must first generate the CA Key pair to be used by the Management Station and the gateway:

- 1 Generate the CA Key for the Management Station using the `fw ca genkey` command as follows:

```
fw ca genkey "[-ou] [-o] [-c]"
```

where `-ou`, `-o` and `-c` specify the DN of the Certificate Authority.

- 2 Distribute the CA Key to the FireWalled gateway using the `fw ca putkey` command:

```
fw ca putkey <target> [-p password]
```

The parameter `target` is the IP address or resolvable name of the machine on which you are installing the CA key (the FireWalled gateway).

The password will be used to authenticate communication between the Management Station and the gateway. If you do not enter a password, you will be prompted for one.

- 3 Generate a Certificate using the following command:

```
fw certify ssl <management> <target> [-p password]
```

The parameter `management` is the IP address or resolvable name of the gateway's Management station.

You must enter the same password you used when you issued the `fw ca putkey` command.

## Modifying the Security Server Configuration File

You must next modify the file `$FWDIR/conf/fwauthd.conf` by specifying SSL encryption for the HTTP Client Authentication daemon on an additional service port:

```
950      bin/in.ahclientd      wait      950      ssl
```



## Client Authentication

### How the User Connects

In the Web browser, the user initiates an HTTPS session on the gateway. The user must specify the gateway name and the port to which to connect, for example:



FIGURE 1-48 Beginning an encrypted Client Authentication Session

The above example uses port 950, but any unused port number can be specified.

## Security Considerations — Client Authentication

### Timeouts

The Client Authentication authorization period is specified in the **Limits** tab of the **Client Authentication Action Properties** window. When the authorization period for the rule times out, the user must sign on and reauthenticate.

When using HTTP (for example, in a Partially Automatic Sign on rule), the **User Authentication Timeout** period in the **Properties Setup** window also affects the period of time during which the user may work without having to reauthenticate. For HTTP, a one-time password is considered valid for this time period. A user working with HTTP does not have to generate a new password and reauthenticate for each connection. Each successful access resets the User Authentication timeout to zero.

If the User Authentication Timeout period is longer than the Client Authentication timeout, an authorized user with a one-time password can continue working without having to reenter the password, even after the Client Authentication timeout has expired. This is because the browser automatically re-sends the password for each connection. If the user initiates an HTTP connection after the Client Authentication authorization times out, the browser automatically sends the previously used password. If the User Authentication period has not timed out, then the password is still valid.

## Client Authentication — Additional Features

### Authorizing All Standard Sign On Rules

By default, the automatic sign on methods (Partially or Fully Automatic) open one rule after successful authentication — the rule for which the sign on was initiated. For example, if a user successfully authenticates according an automatic sign on rule, that user is allowed to work with the services and destinations permitted only by that rule.

You can configure FireWall-1 to automatically open all Standard Sign On rules after successful authentication through Partially or Fully Automatic Sign On. If a user successfully authenticates according to an automatic sign on rule, then all Standard Sign On rules which specify that user and source are opened. The user is then

## Client Authentication — Additional Features

permitted to work with all the services and destinations permitted by the relevant rules. In other words, FireWall-1 knows which user is on the client, and additional authentication is not necessary.

To authorize all relevant Standard Sign On Rules after successful Partially or Fully Automatic authentication, set the `automatically_open_ca_rules` property in the file `objects.C` to `true`. The new value will take effect after you install the Security Policy.

### Changing the Client Authentication Port Number

To change the port number used for the Client authentication feature, proceed as follows:

- 1 Stop FireWall-1 (`fwstop`).
- 2 Modify the port number in the **TCP Services Property** window for the following services:
  - If you want to modify the port number for TELNET sign on, then modify the port number of the `FW1_clntauth_telnet` service.
  - If you want to modify the port number for HTTP sign on, then modify the port number of the `FW1_clntauth_http` service.

These services are special FireWall-1 services provided as part of the Client Authentication feature.
- 3 In the file `$FWDIR/conf/fwauthd.conf`, change the port number for the Client Authentication daemon to the same port number as in the previous step.
  - For TELNET sign-on, modify the `in.aclientd` line.
  - For HTTP sign-on, modify the `in.ahclientd` line.

```
21 bin/in.ftp      wait 0
80 bin/in.ahhttpd  wait 0
513 bin/in.arlogind wait 0
25 bin/in.asmtpd   wait 0
23 bin/in.atelnetd wait 0
259 bin/in.aclientd wait 259
900 bin/in.ahclientd wait 900
10081 bin/in.lhttpd wait 0
```

FIGURE 1-49 `$FWDIR/conf/fwauthd.conf` file



Warning – Do not change anything else in the line.

## Client Authentication

For a description of the fields in this file, see "Security Server Configuration" on page 123.

- 4 Make sure that there is no rule that blocks the connection to the new port.
- 5 Restart FireWall-1 (fwstart).

Not all of the parameters shown in the sample file above will necessarily be present in your file.

## Single Sign-on System Extension

The Single Sign On System Extension to Client Authentication enables a privileged user to sign on and sign off on behalf of other users. The privileged user does not necessarily have to be a person, but can also be an application that enables special access privileges to users based on data in its own database. Consider the following configuration and Rule Base.

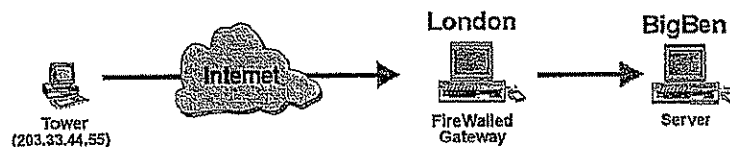


FIGURE 1-50 Single Sign On Extension.

Source	Destination	Services	Action	Track	Install On
All_Users@Any	BigBen	telnet, ftp	Client Auth	Long Log	Gateways

A user on Tower would, in the usual case, TELNET to port 259 on London and authenticate himself or herself, and then request access to BigBen. With the Single Sign On System Extension, another user can open the connection to BigBen in advance on behalf of a user on Tower.

The system administrator must define a user named "sso-root". sso-root must be given Client Authenticated TELNET access to London. sso-root can then open and close connections on behalf of other users as follows:

- 1 sso-root TELNETs to port 259 on London and authenticates himself (or herself).  
It makes no difference from which machine sso-root TELNETs to London.
- 2 After the authentication is successful, the following prompt appears:

```
[real-name@]real source:
```

This prompt appears because the user's name is "sso-root".

## Client Authentication — Additional Features

- 3 sso-root now enters the name and client of another user for whom access is to be allowed, for example:

```
[real-name@]real source:lisa@tower
```

or

```
[real-name@]real source:lisa@203.33.44.55
```

- 4 Next, sso-root must choose (on behalf of lisa):

```
Choose:
(1) Standard Sign-on
(2) Sign-off
(3) Specific Sign-on
```

- 5 From this point on, lisa on the host tower (IP address 203.33.44.55) can TELNET or FTP to BigBen (under the rule shown above) without having to first authenticate herself on London.

If sso-root had entered only the client name (in step 3 above), then all users on tower with open Client Authenticated sessions would have been immediately signed off.

#### Example

Suppose an ISP wishes to make a special service available only to dial-up customers who have paid an additional fee. One way to accomplish this is as follows:

- 1 Define a rule allowing access to the service only after Client Authentication.

Source	Destination	Services	Action	Track	Install On
All_Users@Any.	special server	special service	Client Auth	Long Log	Gateways

- 2 After a customer dials in, gains access to the ISP and is assigned an IP address (presumably after some authentication procedure), a user-written application determines whether the customer is authorized to use the special service.

## Client Authentication

- 3 If the customer is authorized to use the special service, a user-written application TELNETs to port 259 on the FireWall and authenticates itself as follows:

parameter	value
user	ss0-root
password	ss0-root's password
{real-name@}real source:	customer@dynamically-assigned IP address

From this point on, the customer can access the special service without undergoing any additional authentication procedures.

- 4 When the customer logs off from the ISP (or if the dial-up connection drops), the user-written application signs the client off.

The user-written application TELNETs to port 259 on the FireWall and authenticates itself as follows:

parameter	value
user	ss0-root
password	ss0-root's password
{real-name@}real source:	dynamically-assigned IP address

CHAPTER **2**

# Security Servers

---

## In This Chapter

<i>Overview</i>	<i>page 101</i>
<i>Security Servers and the Rule Base</i>	<i>page 104</i>
<i>FTP Security Server</i>	<i>page 107</i>
<i>SMTP Security Server</i>	<i>page 109</i>
<i>HTTP Security Server</i>	<i>page 112</i>
<i>Interaction with OPSEC Products</i>	<i>page 120</i>
<i>Defining Security Servers</i>	<i>page 122</i>

## Overview

When the first packet of a new connection arrives at a FireWall (a gateway or host with FireWall-1 installed), the Inspection Module examines the Rule Base to determine whether or not the connection is to be allowed. FireWall-1 applies the first rule that describes the connection (**Source**, **Destination** and **Service**); if this rule's **Action** is **Accept** or **Encrypt**, then the connection is allowed.

Once a connection is established, FireWall-1 adds the connection to the connections table. Subsequent packets of the connection are verified against the connections table rather than against the Rule Base. The packet is allowed to pass only if the connection is listed in the connections table.

## Overview

In a connection such as this, the entire connection is handled by the FireWall-1 Kernel Module (FIGURE 2-1).

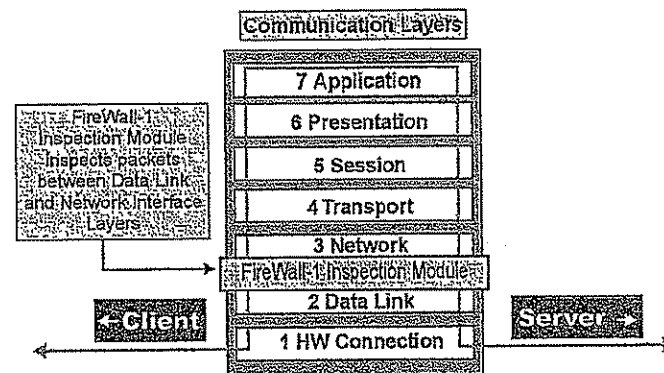


FIGURE 2-1 A connection handled by the FireWall-1 Kernel Module

When the relevant rule specifies a **Resource** under **Service**, or **User Authentication** under **Action**, the corresponding FireWall-1 Security Server is invoked in order to mediate the connection (FIGURE 2-2).

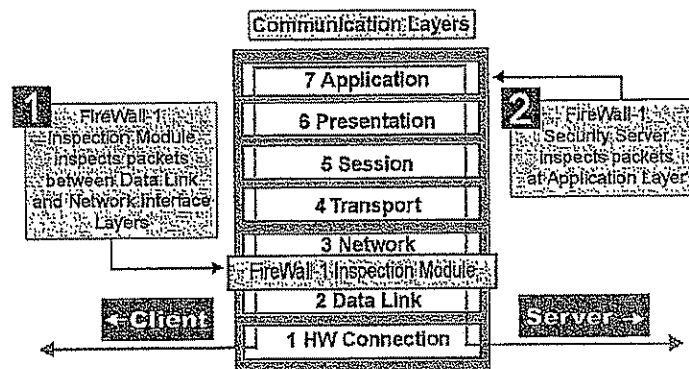


FIGURE 2-2 A connection mediated by a FireWall-1 Security Server

The FireWall-1 Security Servers provide two features:

**1 Authentication**

For information about Authentication, see Chapter 1, "Authentication."

**2 Content Security**

For information about Content Security, see Chapter 3, "Content Security."



When a FireWall-1 Security Server is invoked, the Kernel Module diverts all the packets in the connection to the Security Server, which performs the required authentication and/or Content Security inspection. If the connection is allowed, then the Security Server opens a second connection to the final destination. Altogether, there are two connections: one from the client to the Security Server, and another from the Security Server to the final destination (the server, from the client's point of view). Both of these connections are maintained in the connections table.

There are five FireWall-1 Security Servers, as described in TABLE 2-1.

**TABLE 2-1** FireWall-1 Security Servers — features

Server	Authentication	Content Security	Comments
TELNET	yes	no	
RLOGIN	yes	no	
FTP	yes	yes	
HTTP	yes	yes	
SMTP	no	yes	secure sendmail

#### TELNET

The TELNET Security Server provides Authentication services, but not Content Security.

#### RLOGIN

The RLOGIN Security Server provides Authentication services, but not Content Security.

#### FTP

The FTP Security Server provides Authentication services, and Content Security based on FTP commands (PUT/GET), file name restrictions, and CVP checking (for example, for viruses).

In addition, the FTP Security Server logs FTP get and put commands, as well as the associated file names, if the rule's **Track** is **Long Log**.

#### HTTP

The HTTP Security Server provides Authentication services, and Content Security based on schemes (HTTP, FTP, GOPHER etc.), methods (GET, POST, etc.), hosts (for example, "\*.com"), paths and queries. Alternatively, a file containing a list of IP addresses and paths to which access will be denied or allowed can be specified.

#### SMTP

The SMTP Security Server provides Content Security based on **From** and **To** fields in the envelope and header and attachment types. In addition, it provides a secure sendmail application that prevents direct online connection attacks.



## Security Servers and the Rule Base

The SMTP Security Server also serves as an SMTP address translator, that is, it can hide real user names from the outside world by rewriting the **From** field, while maintaining connectivity by restoring the correct addresses in the response.

## Security Servers and the Rule Base

## The 'Insufficient Information' Problem

At the time the Rule Base is examined, it is not always possible for FireWall-1 to know which rule applies to a connection. This is because the connection's first packet, on the basis of which FireWall-1 must determine whether to allow or disallow the connection, does not contain all the information FireWall-1 needs in order to determine which rule applies to the connection.

For example, consider the following network configuration and Rule Base:

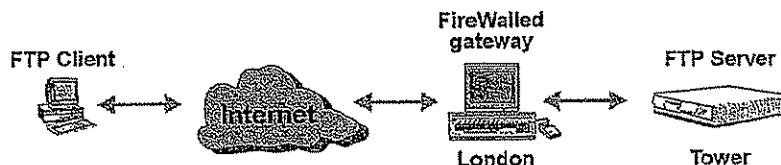


FIGURE 2-3 Protected FTP Server

Source	Destination	Services	Action	Track	Install On
Professors@Any	tower	ftp	UserAuth	Short Log	Gateways
Any	tower	ftp->GetResource	Accept	Long Log	Gateways
Any	Any	Any	Reject	Long Log	Gateways

Suppose the user Alice FTPs to Tower. Should FireWall-1 authenticate her (in accordance with the first rule) or accept the connection without authentication (in accordance with the second rule)? The answer depends on whether Alice belongs to the group **Professors@Any**, but FireWall-1 can only find out who she is (and on the basis of who she is, to which user groups she belongs) by invoking the Authentication process.

However, FireWall-1 cannot first authenticate Alice (to find out who she is) and then decide which rule to apply, because this can lead to the absurd situation where a user fails the Authentication process but the connection is still allowed.

## The Solution

The FireWall-1 Authentication procedure, depicted in FIGURE 2-4 on page 106, solves this problem. The procedure prevents an Authentication rule from being applied when another less restrictive rule (that is, a rule without Authentication) can also be applied to the connection.

The Solution

**Examples**

Consider the following Rule Base:

Source	Destination	Services	Action	Track	Install On
Professors@Any	tower	ftp	UserAuth	Short Log	Gateways
Teachers@Any	tower	ftp->GetResource	UserAuth	Long Log	Gateways
Any	Any	Any	Reject	Long Log	Gateways

Suppose a user FTPs to Tower. FireWall-1 matches the first rule, and invokes the FTP Security Server and authentication process. However, if the user belongs to Teachers@Any, then the second rule is the one which applies to the connection. Since both rules specify Authentication, it doesn't matter that the Authentication was invoked by a rule other than the one that was applied to the connection. This is because Authentication scheme and password are attributes of the user, not of the group, and are the same whether the user is being authenticated as a member of Professors@Any or of Teachers@Any.

## Security Servers and the Rule Base

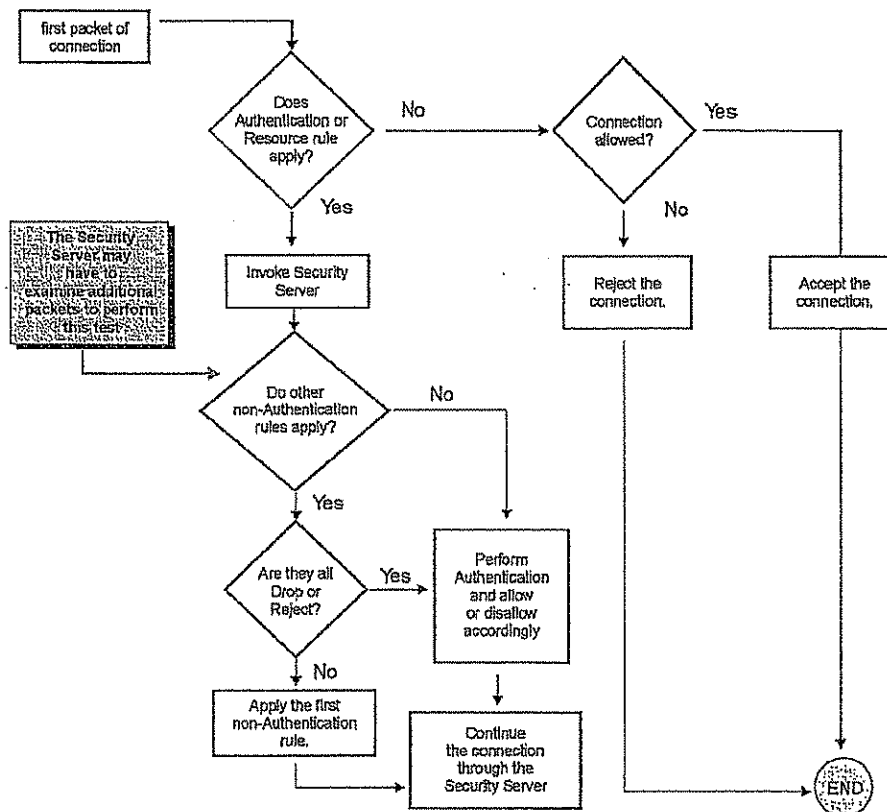


FIGURE 2-4 Authentication Procedure

Next, consider this Rule Base:

Source	Destination	Services	Action	Track	Install On
Professors@Any	tower	ftp	UserAuth	Short Log	Gateways
Any	tower	ftp->GetResource	Accept	Long Log	Gateways
Any	Any	Any	Reject	Long Log	Gateways

### Outgoing Connections

Suppose a user FTPs to Tower. The first matching rule is the first rule (whose **Action** is **UserAuth**), but it is the second rule which is applied, because it also matches but its **Action** is **Accept**. In this case, it is important that the original rule was not applied, that is, that there was no Authentication even though the Security Server was invoked.



**Note** – In this case, the connection is mediated by the Security Server, even though there was no Authentication.

You can verify this by stepping through the Authentication procedure depicted in FIGURE 2-4 on page 106.

### Outgoing Connections

User Authentication and Resource rules are applied only to connections incoming to a FireWalled machine. An outgoing connection originating on a FireWalled machine will not be folded into a Security Server on that machine, but will be dropped.

### FTP Security Server

When an FTP connection is mediated by the FireWall-1 FTP Security Server, then the user's requested FTP commands and file names are matched against the FTP Resource defined in the relevant rule.

The FTP Security Server is invoked when a rule specifies an FTP Resource in the **Service** field and/or User Authentication in the **Action** field. If no FTP Resource is specified in the rule (that is, if the Security Server is invoked because the **Action** is User Authentication), then an FTP Resource of GET and PUT allowed for all files is applied.

## Security Servers and the Rule Base

**FTP Resource Matching**

FTP Resource matching consists of matching methods and file names.

**Methods**

TABLE 2-2 lists the FTP commands that correspond to the methods specified in the FTP Resource definition.

**TABLE 2-2** FTP actions and commands

method (defined in the FTP Resource)	applies to these FTP commands	meaning
GET	RETR	retrieve
	RNFR	rename from
	XMD5	MD5 signature
PUT	STOR	store
	STOU	store unique
	APPE	append
	RNFR	rename from
	RNTO	rename to
	DELE	delete
	MKD	make directory
	RMD	remove directory

The FireWall-1 FTP Security Server passes all other FTP commands to the FTP server for execution.

**File Names**

File name matching is based on the concatenation of the file name in the command and the current working directory (unless the file name is already a full path name) and comparing the result to the path specified in the FTP Resource definition.

When specifying the path name in the FTP Resource definition, only lower case characters and a directory separator character / can be used.

The Security Server modifies the file name in the command as follows:

- for DOS, the drive letter and the colon (:) is stripped for relative paths
- the directory separator character (/ or \) is replaced, if necessary, with the one appropriate to the FTP server's OS

In some cases, the Security Server is unable to resolve the file name, that is, it is unable to determine whether the file name in the command matches the file name in the resource.

## SMTP Security Server

## Example - DOS

Suppose the current directory is d:\temp and the file name in the resource is c:x. Then the Security Server is unable to determine the absolute path of the file name in the command because the current directory known to the Security Server is on disk D: and the file is on disk c:, which may have a different current directory.

## Example - Unix

If the file name in the command contains . . references which refer to symbolic links, then it's possible that the file name in the command matches the resource's path, but that the two in fact refer to different files.

When the Security Server cannot resolve a file name, the action it takes depends on the **Action** specified in the rule being applied:

- If the rule's **Action** is Reject or Drop, then the rule is applied and its **Action** taken.
- If the rule's **Action** is Accept, Encrypt or Authenticate, then:

If the resource path is \* or there is no resource, the rule is applied.

Otherwise, the rule is not applied. Instead, FireWall-1 scans the Rule Base and applies the next matching rule (which may be the default rule that drops everything). In this case, a potential problem is that the rules may specify different entries in their **Track** fields. For example, it may happen that the original rule specifies **Accounting** in the **Track** field while the rule that is applied does not.

## SMTP Security Server

The SMTP Security Server does not provide Authentication, because there is no human user at a keyboard who can be challenged for authentication data. However, the SMTP Security Server provides Content Security that enables a Security Administrator to:

- provide mail address translation by hiding outgoing mail's **From** address behind a standard generic address that conceals internal network structure and real internal users
- drop mail from given addresses
- strip MIME attachments of specified types from mail
- strip the **Received** information from outgoing mail, in order to conceal internal network structure
- drop mail messages above a given size
- CVP checking (for example, for viruses)



### Security Servers and the Rule Base

In addition, the SMTP Security Server provides additional security over standard sendmail applications. Its functionality is split between two separate modules (FIGURE 2-5), so there is no direct path connecting mail servers, preventing direct online connections to the real sendmail application.

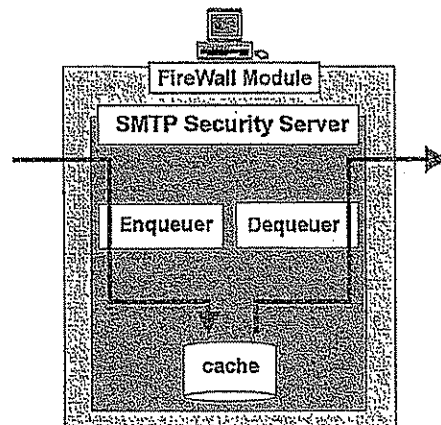


FIGURE 2-5 FireWall-1 SMTP Security Server

One process writes incoming messages to a disk cache, and the other process empties the cache.

### Functionality

The FireWall-1 SMTP Security Server supports the following SMTP commands:

- |        |        |        |
|--------|--------|--------|
| ■ RCPT | ■ QUIT | ■ HELP |
| ■ MAIL | ■ DATA | ■ RSET |
| ■ HELO | ■ NOOP | ■ VRFY |

The VRFY command always returns USEROK, to prevent repeated messages from automatic mailers.

## SMTP Security Server

## SMTP Security Server Configuration

The SMTP Security Server configuration file is `$FWDIR/conf/smtp.conf`.

TABLE 2-3 Fields in `$FWDIR/conf/smtp.conf`

parameter	meaning
timeout	number of seconds after which connection times out
scan_period	how frequently the spool directory is scanned
resend_period	number of seconds after which the SMTP Security Server resends the message after failing to deliver the message
abandon	number of seconds after which the SMTP Security Server abandons attempts to resend
rundir	SMTP Security Server files are written at and below this directory
postmaster	to whom to send error messages
default_server	the actual sendmail application resides here
error_server	the server to be notified in the event of an error

## Alerts

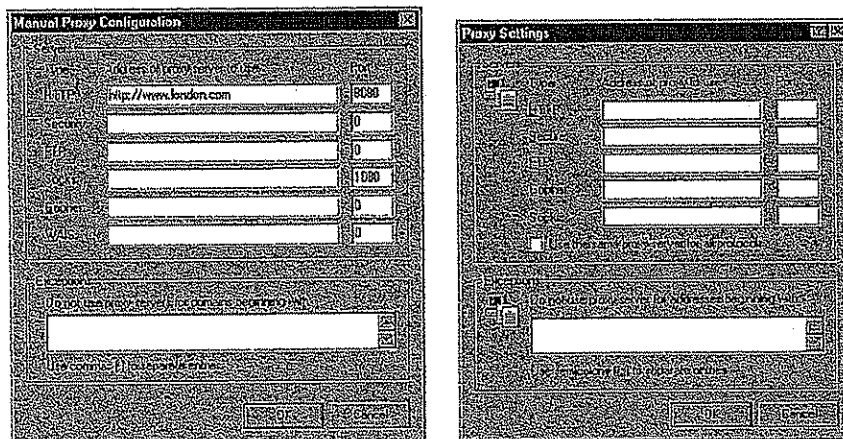
The SMTP Security Server can be configured to issue alerts in the event of various SMTP-related system error conditions, such as insufficient disk space (possibly caused by a denial-of-service attack).

## Security Servers and the Rule Base

**HTTP Security Server****Support for FTP**

The HTTP Security Server supports FTP requests through a web browser. The HTTP Security Server must be defined as the HTTP proxy to the user's Web browser. This is done in the user's Web browser proxy settings.

FIGURE 2-6 shows the proxy configuration windows for Netscape and Internet Explorer.



**FIGURE 2-6** Proxy Configuration — Netscape 4.0 and Internet Explorer 3.0x

When a user requests an FTP URL through a browser:

- 1 The browser connects to the Security Server and sends an HTTP request with FTP as the method.
- 2 The Security Server opens an FTP session with the requested server.
- 3 The Security Server sends the FTP request to the server and formats all responses as HTTP messages, which it sends to the browser. These messages are listed in the file /conf/f2ht-msgs.

The Security Server sends a RETR request to the FTP server to determine whether the requested URL specifies a directory or plain file. If the FTP server returns an error message with a text line indicating the request is not a plain file, the Security Server assumes the requested URL is a directory. The Security Server then sends the directory listing to the browser as an HTML page.

If the requested URL is a file, the Security Server determines whether it is a text file or a binary file. If the requested file ends with one of the suffixes listed in the file /conf/f2ht-bin-sfxs, it is considered a binary file.

## HTTP Security Server

FTP requests through a web browser are enabled by both User Authentication and URI Resource rules. If the relevant rule specifies a URI Resource, then **ftp** must be defined as one of the enabled Schemes in the **URI Definition** window.

For more information on URI Resources, see Chapter 6, "Resources" in *Managing FireWall-1 Using the Windows GUI* or *Managing FireWall-1 Using the OpenLook GUI*.

**Support for HTTPS**

HTTPS (HTTP encrypted by SSL) connections are handled by the HTTP Security Server in the following ways:

- **Security Proxy Mode** — In Security Proxy mode, the HTTP Security Server is defined as the "security proxy" in the user's Web browser settings. The HTTP Security Server acts as a proxy for HTTPS connections, but does not inspect content.
- **Non-transparent Mode** — The HTTP Security Server is configured to encrypt and decrypt HTTPS connections. This option is known as "Non-transparent", because the user of HTTPS must initiate the connection on the gateway before connecting to the target server.

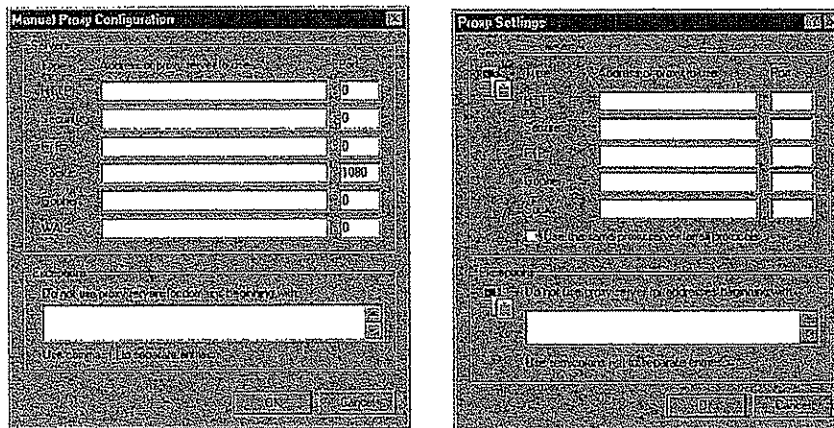
**Security Proxy Mode**

HTTPS (HTTP encrypted by SSL) connections can be handled by the HTTP Security Server when it is defined as the Security Proxy to the local user's Web browser. The HTTP Security Server proxies outgoing HTTPS connections, but does not inspect content. This option can be used with User Authentication rules to authenticate outgoing HTTPS, and with Resource rules. User Authentication and Resource rules can be used together.

The user can configure a Security Proxy for the following Web browsers:

- Internet Explorer version 3.0x and higher
- Netscape version 4.0x and higher

## Security Servers and the Rule Base



**FIGURE 2-7** HTTP Proxy and Security Proxy Settings — Netscape 4.0x and Internet Explorer 3.0x

HTTPS requests generally use the HTTP "CONNECT" method (tunneling mode). Because the CONNECT method only specifies a hostname and port, the HTTP Security Server does not have access to the content of the communication, not even the URL. In addition, the Security Server does not verify that the connections are really using HTTPS — it only checks the requested hostname and port number. All communication between the client and the target server is encrypted — the HTTP Security Server mediates the connection. This is useful if internal users want to send encrypted information over the Internet.



**Note** — Although the connection is encrypted between the local client and the external server, the authentication session between the local client and the HTTP Security Server is clear (unencrypted).

#### User Authentication Rules

In Security Proxy mode, you can provide security by requiring internal users to authenticate before accessing external HTTPS servers.

To authenticate users of outgoing HTTPS, proceed as follows:

- 1 Internal users must define the HTTP Security Server as the Security Proxy on port 443. This is done in the proxy settings of the user's Web browser (FIGURE 2-7 on page 114).



## HTTP Security Server

- 2 Add the following line to the file `$FWDIR/conf/fwauthd.conf`:

```
443 bin/in.ahhttpd wait 0
```

This enables the HTTP Security Server to run on the port specified for the Security Proxy.

- 3 In the HTTPS service properties, set the **Protocol Type** to **URI** (FIGURE 2-8). This assures that the HTTPS service (using port 443) will be mediated by the HTTP Security Server.

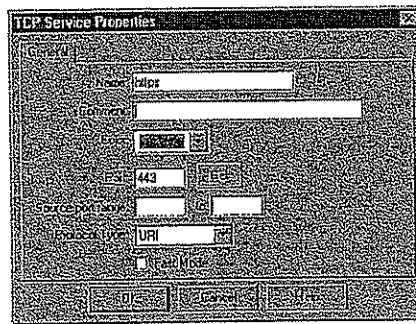


FIGURE 2-8 HTTPS Service Definition

- 4 Define a rule similar to the following

Source	Destination	Services	Action	Track	Install On
All_Users@localnet	any	https	UserAuth	Long Log	Gateways

According to this rule, internal users must authenticate before accessing external HTTPS.

- 5 In the rule's **User Authentication Action Properties** window, check **All Servers** under **HTTP**. This assures that the outgoing connections will be allowed to continue from the HTTP Security Server to any external host or port.



## Security Servers and the Rule Base

### URI Resource rules

The **URI Definition** window must specify the following:

#### Connection Methods — check Tunneling

When **Tunneling** is checked, HTTP requests using the **CONNECT** method are matched. The HTTP Security Server does not inspect the content of the request, not even the URL. Only the host and port number can be checked. Therefore, when **Tunneling** is checked, some Content Security options in the URI Resource specification, (for example, CVP options, HTML weeding) are disabled.

If you check **Tunneling**, you may still use the URI File or UFP specifications. A URI File specification must define a file that lists only server names and their port numbers. The UFP specification must use a UFP server that maintains a list of only server names and port numbers.

**Host** — Specify the host and port of a known HTTPS server, for example:

```
https server host:443
```

The field to the left of the colon specifies the URI's host. The field to the right of the colon specifies the port. A wildcard character (\*) indicates any host.

For more information on URI Resources, see Chapter 6, "Resources" in *Managing FireWall-1 Using the Windows GUI* or *Managing FireWall-1 Using the OpenLook GUI*.

### Non-transparent Mode and HTTPS

If you are implementing Non-transparent Authentication, the HTTP Security Server can be configured to encrypt and decrypt HTTPS connections. This option enables the HTTP Security Server to inspect the contents of HTTPS connections.

The connection can be encrypted between the client and the HTTP Security Server, and then possibly again from the HTTP Security Server to the target server. For example, you can specify that connections between the client and HTTP Security Server are encrypted. The HTTP Security Server on the gateway decrypts and inspects the connection. The connection can then be encrypted again from the HTTP Security Server to the target host. The authentication session is encrypted as well.

This option is known as "Non-transparent Mode" because the user of HTTPS must request the gateway before being allowed to continue to the target host. Because the HTTP Security Server is not defined as a Security Proxy to the user's Web browser, Non-transparent Mode is best used to authenticate external users accessing internal servers.

To configure support for HTTPS, proceed as follows:

## HTTP Security Server

## Enabling Non-transparent Authentication

FireWall-1 Version 4.0 by default implements transparent authentication, in which the user can directly connect to the target server. To configure the HTTP Security Server to encrypt and decrypt HTTPS, you must enable Non-transparent Authentication, in which the user connects to the gateway before continuing on to the target server.

To enable Non-transparent Authentication:

- 1 In the objects.C file, set the `prompt_for_destination` parameter to true.

This value indicates that if the user requests the gateway as the destination, the FireWall Module assumes the user's "true" destination is some other server, and prompts the user for the "true" destination.

For more information on Non-transparent Authentication see:

- "Non-Transparent User Authentication" in Chapter 1, "Authentication"
- "HTTP Security Server and Non-Transparent Authentication" in Chapter 1, "Authentication"

## Generating CA Keys

Next, you must first generate the CA Key pair to be used by the FireWall-1 Management Station and the gateway.

- 2 Generate the CA Key for the Management Station by using the `fw ca genkey` command as follows:

```
fw ca genkey "[-ou] [-o] [-c]"
```

where `-ou`, `-o`, and `-c` specify the Distinguished Name (DN) of the Certificate Authority.

- 3 Distribute the CA Key to the FireWalled gateway using the `fw ca putkey` command.

```
fw ca putkey <target> [-p password]
```

The parameter `target` is the IP address or resolvable name of the machine on which you are installing the CA key (the FireWalled gateway).

The parameter `-p password` is a password that will be used to authenticate future communication between the Management Station and the gateway.

If you do not enter a password, you will be prompted for one.

## Security Servers and the Rule Base

- 4 Generate a Certificate using the following command:

```
fw certify ssl <management> <target> [-p password]
```

The parameter management is the IP address or resolvable name of the gateway's Management station.

You must enter the same password you used when you issued the `fw ca putkey` command in step 3.

## Modifying the Security Server Configuration File

- 5 You must next modify the file `$FWDIR/conf/fwauthd.conf` by adding a line which enables the HTTP Security Server to run on an additional service port dedicated to HTTPS. According to the example below, HTTPS connections will connect to the gateway on port 443.

Example:

```
443 bin/in.ahttpd wait 0 ec
```

The last field specifies what to do with HTTPS (SSL) connections. TABLE 2-4 lists the available options:

TABLE 2-4 HTTPS options

option	meaning
ec	encrypt connections between the client and the gateway
es	encrypt connections between the gateway and the server
eb	encrypt both — encrypt connections between the client and the gateway, and then between the gateway and the server.
ns	no SSL (no encryption)

Leaving this field empty is the same as specifying ns.

For more information about the file `$FWDIR/conf/fwauthd.conf`, see "Security Server Configuration" on page 123.

## HTTP Servers

- 6 You must also define the HTTP servers to which HTTPS connections are allowed.

HTTP servers are defined in the **HTTP Server Definition** window (FIGURE 2-9). For information on defining HTTP servers, see "Configuring HTTP Servers" in Chapter 1, "Authentication".

## HTTP Security Server

## Example

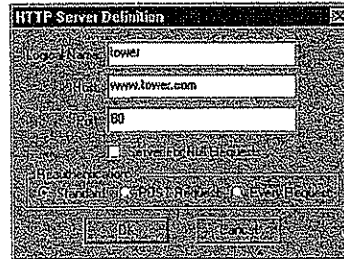


FIGURE 2-9 Example HTTP Server definition

You must specify the **Logical Name**, **Host** and **Port** number on which you installed the servers which will handle HTTPS connections.

## HTTPS Service Properties

- 7** You must next modify HTTPS properties to assure that the service will be mediated by the HTTP Security Server. In the HTTPS service definition, set the **Protocol Type** to **URI** (see FIGURE 2-8 on page 115).

## User Authentication Rule

- 8** Next, define a rule similar to the following:

Source	Destination	Services	Action	Track	Install On
All_Users@any	localnet	https	UserAuth	Long Log	Gateways

In the rule's **User Authentication Action Properties** window, specify **Predefined Servers** under **HTTP**. This restricts incoming HTTPS to the servers listed in the **Security Servers** tab of the **Properties Setup** window (the HTTP Servers you defined in step 6 on page 118 ).

## How the User Connects

An external user of HTTP must specify the name of the FireWalled gateway and the logical name of the target server in the requested URL. This assures that the request will be intercepted by the HTTP Security Server on the gateway. The URL is set up as follows:

```
https://<gateway_name>/<logical_server_name>/...
```

#### Interaction with OPSEC Products

For example, if the gateway name is London, and the target server (behind London) is Tower, then the user specifies the following URL:

```
https://www.london.com/tower/...
```

For information on how to set up URLs for Non-transparent Authentication, see "Configuring URLs" in Chapter 1, "Authentication".

### Interaction with OPSEC Products

The FireWall-1 Security Servers support third-party products working with Check Point's OPSEC SDK. In the OPSEC framework, the enterprise security system is composed of several components, each of which is provided by different a different vendor and may be installed on a different machine. FireWall-1 distributes security tasks to the OPSEC components. Transactions between FireWall-1 and OPSEC security components take place using open, industry standard protocols.

Information about OPSEC is available at [www.opsec.com](http://www.opsec.com).

Example OPSEC components are:

- a CVP (Content Vectoring Protocol) server that examines files for content
- a UFP (URL Filtering Protocol) server that categorizes URLs

In a common OPSEC model, a FireWall-1 Security Server acts as a client sending requests to an OPSEC server. The Security Server intercepts a connection and generates a request to the OPSEC server. The server processes the request and sends a reply to the Security Server, which processes the original connection based on the reply.

HTTP Security Server

FIGURE 2-10 shows how the HTTP Security Server handles a connection request to a URL:

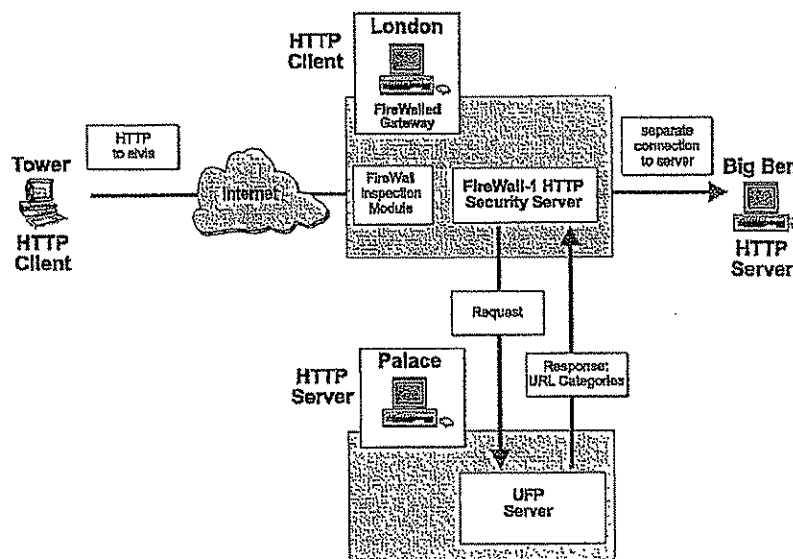


FIGURE 2-10 Connection invoking a UFP Server

**1** Firewall-1 intercepts a connection request to a URL.

The connection matches a rule which specifies a URI Resource under the Rule Base Service field. The Resource definition specifies a UFP server which maintains a list of URLs and their categories. Firewall-1 determines that the UFP server must be invoked.

**2** Firewall-1 diverts the connection to the HTTP Security Server. The Security Server connects to the UFP server and initiates the URL Filtering Protocol.

**3** The HTTP Security Server sends a request containing the name of the URL.

**4** The UFP server checks the URL against lists of URLs and their categories. The UFP server returns a message notifying the HTTP Security Server of the categories to which the URL belongs.

**5** The HTTP Security Server takes the action defined for the resource, either allowing or disallowing the connection attempt.

For information on defining UFP or CVP Servers, see Chapter 5, "Server Objects" in *Managing FireWall-1 Using the Windows GUI* or *Managing FireWall-1 Using the OpenLook GUI*.

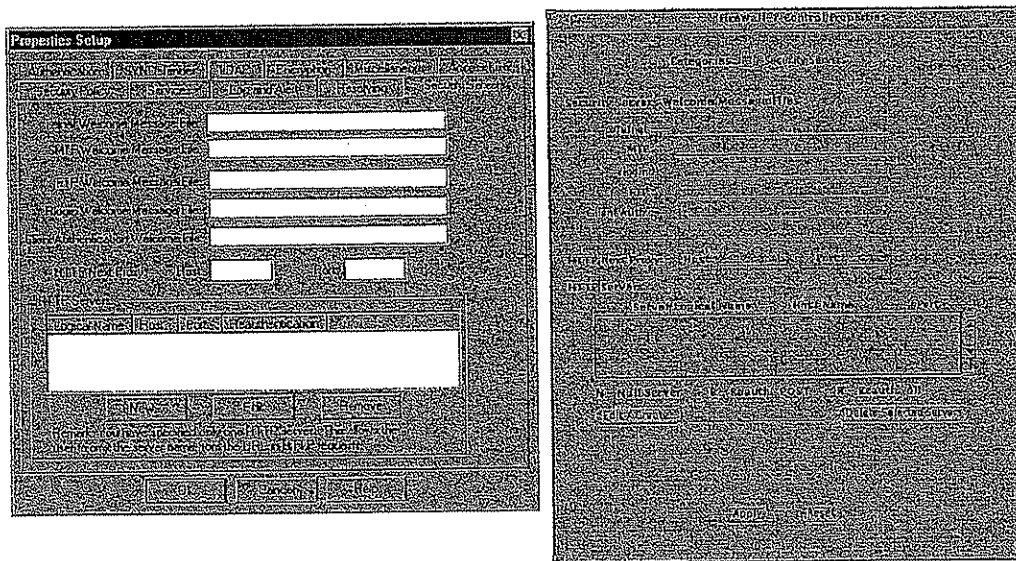


## Defining Security Servers

For more information on OPSEC-certified products see <http://www.opsec.com>.

## Defining Security Servers

The properties of the FireWall-1 Security Servers are specified in the **Security Servers** tab of the **Properties Setup** window in the Windows GUI and in the **Control Properties/Security Servers** window in the OpenLook GUI (FIGURE 2-11).



**FIGURE 2-11** Properties Setup window - Security Servers tab (Windows) and Control Properties/Security Servers window (OpenLook)

**Telnet Welcome Message File** — the name of a file whose contents are to be displayed when a user begins an Authenticated TELNET session (optional)

**SMTP Welcome Message File** — the name of a file whose contents are to be displayed when the SMTP Security Server starts (optional)

**FTP Welcome Message File** — the name of a file whose contents are to be displayed when a user begins an Authenticated FTP session (optional)

**Rlogin Welcome Message File** — the name of a file whose contents are to be displayed when a user begins an Authenticated RLOGIN session (optional)

## Security Server Configuration

**Client Authentication Welcome Message File** — the name of a file whose contents are to be displayed when a user begins a Client Authenticated session (optional)



**Note** — Client Authenticated sessions initiated through the Manual Sign On method are not mediate by a Security Server.

See "Client Authentication" in Chapter 1, "Authentication" for information about Client Authentication.

The following fields specify parameters for the HTTP Security Server:

**HTTP Next Proxy** — For information about this field, see "Caching — Using an HTTP Proxy behind the HTTP Security Server" on page 51 of Chapter 1, "Authentication."

**HTTP Servers** — You can define HTTP Servers to restrict HTTP access to specific hosts and ports. For more information, see "HTTP Servers List (Security Servers tab)" on page 46 of Chapter 1, "Authentication."

## Security Server Configuration

## fwauthd.conf file

Each line in the Security Server configuration file `$FWDIR/conf/fwauthd.conf` corresponds to a Security Server.

21	bin/in.aftpd	wait	0
80	bin/in.ahttpd	wait	0
513	bin/in.arlogind	wait	0
25	bin/in.asmtpd	wait	0
23	bin/in.atelnetd	wait	0
259	bin/in.aclientd	wait	259
900	bin/in.ahclientd	wait	900
10081	bin/in.lhttpd	wait	0

FIGURE 2-12 `$FWDIR/conf/fwauthd.conf` — example

TABLE 2-5 `$FWDIR/conf/fwauthd.conf` fields

field number	meaning
1	standard service's port number
2	Security Server executable
3	wait flag (always set to wait)
4	Security Server port number

## Defining Security Servers

The Security Service executables are listed in TABLE 2-6.

TABLE 2-6 Security Service binaries

Service	binary name
TELNET	bin/in.atelnetd
FTP	bin/in.aftpd
HTTP	bin/in.ahttpd
SMTP	bin/in.asmtpd
RLOGIN	bin/in.arlogind
client authentication	<ul style="list-style-type: none"> <li>■ bin/in.aclientd (This is not a Security Server.)</li> <li>■ bin/in.ahclientd (This is not a Security Server, but the executable for when a user initiates client authentication through a Web browser.)</li> </ul>
logical servers	bin/in.lhttpd (This is not a Security Server.)

The wait flag is always set to wait.

The Security Server port number is one of the following:

- 0 — specifies that FireWall will choose a random high port for the Security Server
  - positive value — specifies a real port number
- If this option is chosen, the standard service's port number (the first field) should be the real port number for the service secured by this Security Server. For example, for TELNET this would usually be port 23.
- negative value — indicates that FireWall-1 randomly chooses multiple ports for the Security Server.

The absolute value indicates the number of random selected ports that will be chosen. The example below specifies that FireWall-1 will randomly select four high ports for the HTTP Security Server:

```
80 bin/in.ahttpd wait -4
```

This option is especially useful for HTTP because it enables several HTTP Security Servers to run concurrently. If you configure a negative port number, the HTTP client will initially connect to a randomly selected port. If the client

## Using a Security Server to Authenticate Other Services

connects again before the **Authorization Timeout** specified in the **Control Properties/Security Servers** window, the same port will be chosen. If the client connects again after the **Authorization Timeout**, another port will be chosen.



**Note** – Configuring a negative port value is recommended only for gateway machines with more than one CPU. Configuring this option on a gateway machine with one CPU can result in a performance degradation.

**Using a Security Server to Authenticate Other Services**

You can use the TELNET, RLOGIN and FTP Security Servers to authenticate any interactive service. The user starts the interactive service as usual, but instead of being immediately connected to the interactive service's server (assuming the Rule Base allows such a connection), the user is first prompted for authentication data by the TELNET Security Server. If the authentication is successful, the user is then connected to the interactive service's server in a normal session.

To do this, add a line in `$FWDIR/conf/fwauthd.conf` as follows:

```
port in.telnetd wait 0
```

where *port* is the normal port for the service you wish to authenticate using the TELNET Security Server.

Defining Security Servers

126 FireWall-1 Architecture and Administration • September 1998

**CHAPTER 3**

# Content Security

## In This Chapter

<i>Overview</i>	<i>page 127</i>
<i>Web (HTTP)</i>	<i>page 130</i>
<i>Mail (SMTP)</i>	<i>page 132</i>
<i>FTP</i>	<i>page 133</i>
<i>CVP Inspection</i>	<i>page 133</i>

## Overview

### Resources and Security Servers

Content Security extends the scope of data inspection to the highest level of a service's protocol, achieving highly tuned access control to network resources. FireWall-1 provides content security for HTTP, SMTP and FTP connections using the Firewall-1 Security Servers and Resource object specifications.

A FireWall-1 Resource specification defines a set of entities which can be accessed by a specific protocol. You can define a Resource based on HTTP, FTP and SMTP. For example, you might define a URI resource whose attributes are a list of URLs and the HTTP and FTP schemes. The resource can be used in the Rule Base in exactly the same way a service can be used, and the standard logging and alerting methods are available to provide monitoring of resource usage.



## Overview

When a rule specifies a Resource in the Service field of the Rule Base, the FireWall-1 Inspection Module diverts all the packets in the connection to the corresponding Security Server, which performs the required Content Security inspection. If the connection is allowed, the Security Server opens a second connection to the final destination.

FIGURE 3-1 depicts what happens when a rule specifies the use of an HTTP Resource.

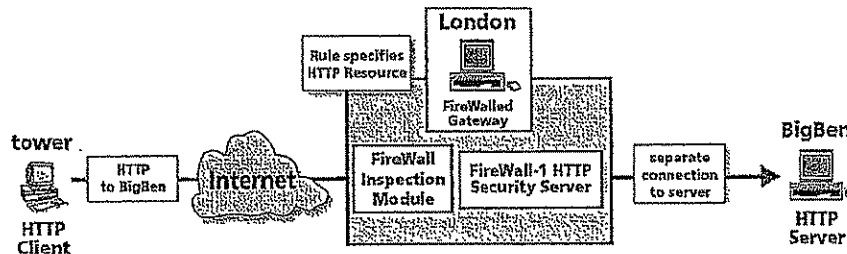


FIGURE 3-1 A connection mediated by the HTTP Security Server

For each connection established through a FireWall-1 Security Server, the Security Administrator is able to control specific access according to fields that belong to the specific service: URLs, file names, FTP PUT/GET commands, type of requests and others. Major security enhancements enabled by the Content Security feature are CVP checking (for example, for viruses) for files transferred and URL filtering.

When a Resource is specified, the Security Server diverts the connection to one of the following servers:

- Content Vectoring Protocol (CVP)

A CVP server examines and reports on the contents of files, for example, whether a file contains a virus.

- URL Filtering Protocol (UFP)

A UFP server maintains a list of URLs and their categories.

The server performs the requested content inspection and returns the results to the Security Server. The Security Server allows or disallows the connection, depending on the results.

Communication between the Security Server and the CVP or UFP server is enabled through Check Point's OPSEC (Open Platform for Secure Enterprise Connectivity) framework. For more information about OPSEC integration within FireWall-1, see <http://www.checkpoint.com/opsec>. If you would like to download evaluation versions of OPSEC-certified products, see <http://www.opsec.com>.

## Resources and Security Servers

FIGURE 3-2 shows what happens when a FireWall-1 Security Server passes a file to a Content Vectoring Server for inspection during an FTP connection.

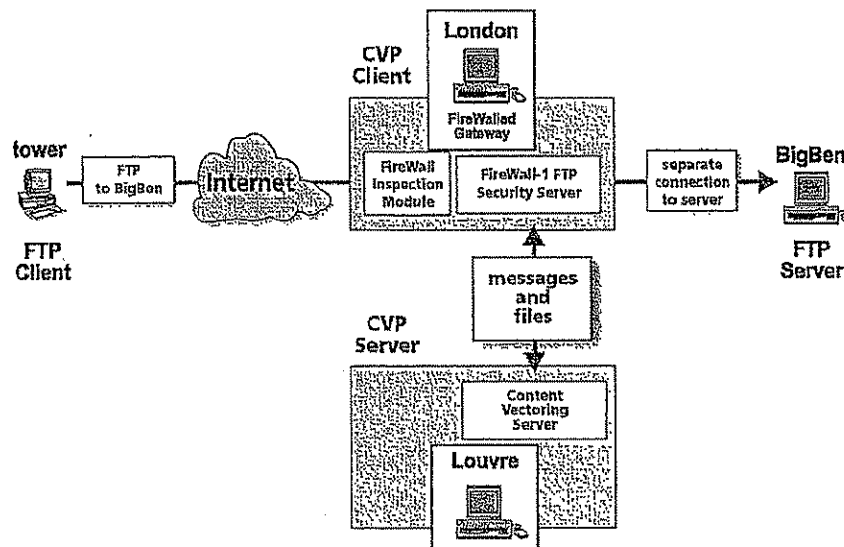


FIGURE 3-2 Content Vectoring Server

- 1 FireWall-1 determines that the Content Vectoring Server must be invoked.  
The relevant rule for the connection specifies a resource which includes CVP checking.
- 2 The FTP Security Server connects to the Content Vectoring Server and initiates the Content Vectoring Protocol.
- 3 The FTP Security Server sends the Content Vectoring Server the file to be inspected.
- 4 The Content Vectoring Server inspects the file, and returns a Validation Result message notifying the FTP Security Server of the result of the inspection.
- 5 The Content Vectoring Server optionally returns a modified version of the file to the FTP Security Server.
- 6 The FTP Security Server takes the action defined for the resource, either allowing or disallowing the file transfer.

For more information on CVP inspection, see "CVP Inspection" on page 133.

Web (HTTP)

## Web (HTTP)

A URI is a Uniform Resource Identifier, of which the familiar URL (Uniform Resource Locator) is a specific case. URI resources can define schemes (HTTP, FTP, GOPHER etc.), methods (GET, POST, etc.), hosts (for example, "\*.com"), paths and queries. Alternatively, a file containing a list of IP addresses of servers and paths can be specified.

In addition, the Security Administrator can define how to handle responses to allowed resources, for example, that JAVA applets not be allowed even on resources that are allowed. JAVA applets, JAVA scripts and ActiveX can be removed from HTML. A customizable replacement URL, for example a page containing a standardized error message, can be displayed when access to a response is denied.

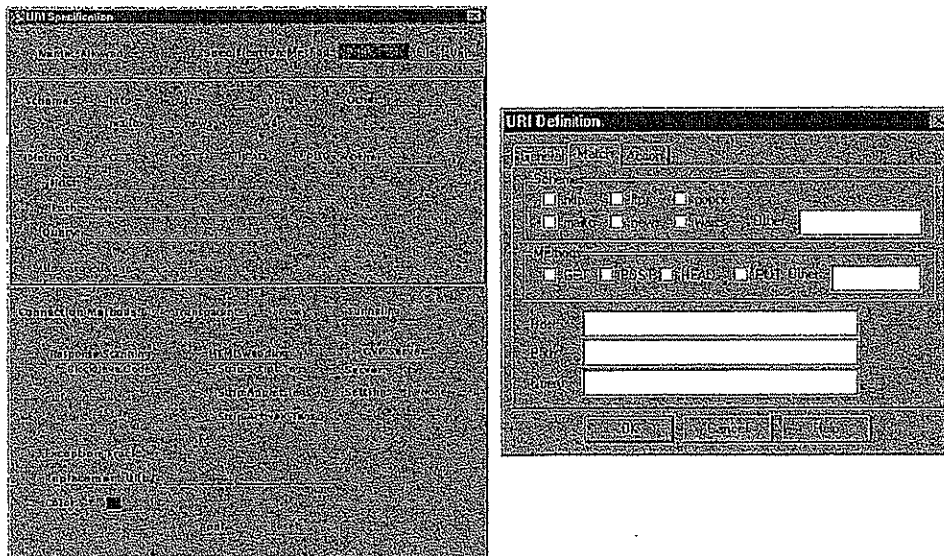


FIGURE 3-3 URI Resource Definition (OpenLook and Windows)

## URL Filtering

URL filtering provides precise control over Web access, allowing administrators to define undesirable or inappropriate Web pages. FireWall-1 checks Web connection attempts using URL Filtering Protocol (UFP) servers. UFP servers maintain lists of URLs and their appropriate categories (i.e. permitted or denied). URL databases can be updated to provide a current list of blocked sites. All communication between FireWall-1 and the URL Filtering server is in accordance with the URL Filtering Protocol.

In order to implement URL filtering, proceed as follows:

- 1 Define a UFP Server.
- 2 Define a URI Resource that specifies a list of URL categories from the UFP server.
- 3 Define rules that specify an action taken for the Resource.

### Defining a UFP Server

UFP Servers are defined in the **UFP Server Properties** window (see Chapter 5, "Server Objects" of *Managing FireWall-1 Using the Windows GUI* or *Managing FireWall-1 Using the OpenLook GUI*).

### Defining a Resource

The URI resource is defined in the **URI Definition** window (UFP Specification). The URI Resource specifies the UFP server and a list of URL categories provided by the server. In the Resource depicted in FIGURE 3-4 on page 131, "WebCop" is the UFP Server, and the URL categories are "alcohol" and "drugs." The "alcohol" category is selected. This means that if WebCop assigns the category "alcohol" to a URL, then the URL matches the resource's definition, and the rule is applied.

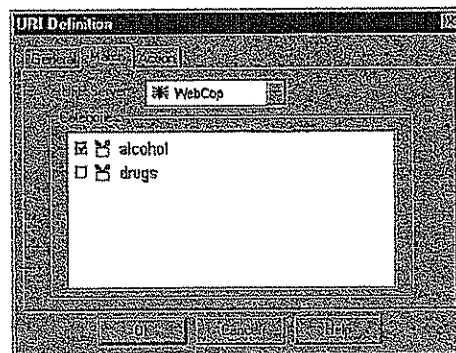


FIGURE 3-4 URI Definition window — Match tab (UFP specification)

### Defining Rules

For example, suppose the Security Administrator defines two URI resources:

- **Allowed** — HTTP and FTP schemes, GET and POST methods
- **NotAllowed** — a list of "forbidden" URLs categories

## Mail (SMTP)

Then the following rules prevent local users from accessing the **NotAllowed** resource and allow users access to the **Allowed** resource after authentication.

No.	Source	Destination	Service	Action	Track	Install On
1	Any	Any	Any	Deny	Alert	Gateways
2	Any	Any	Any	Allow	Alert	Gateways
3	Any	Any	Any	Reject	Alert	Gateways

FIGURE 3-5 Rule Base using Resources

When a Resource in a rule specifies a list of permitted or denied URLs, the HTTP Security Server sends a request to the UFP server containing the name of the URL in question. The UFP server checks the URL against lists of URLs and their categories. The UFP server returns a message notifying the HTTP Security Server of the categories to which the URL belongs.

For example, if a user requests a connection to a URL that belongs to a category specified in the Resource denied HTTP, FireWall-1 denies the connection request. If the URL does not belong to the categories defined by this Resource, the Security Server opens a separate connection to the destination.

For information on defining URI resources, see Chapter 6, "Resources," of *Managing FireWall-1 Using the Windows GUI* or *Managing FireWall-1 Using the OpenLook GUI*.

## Mail (SMTP)

The SMTP protocol, designed to provide maximum connectivity between people all over the Internet, and enhanced to support file attachments, poses a challenge to the Security Administrator who wants to maintain connectivity but keep intruders out of the internal networks.

FireWall-1 offers an SMTP server that provides highly granular control over SMTP connections. The Security Administrator can:

- hide outgoing mail's **From** address behind a standard generic address that conceals internal network structure and real internal users
- redirect mail sent to given **To** addresses (for example, to root) to another mail address
- drop mail from given addresses
- strip MIME attachments of given types from mail
- drop mail messages above a given size

For information on defining SMTP resources, see Chapter 6, "Resources," of *Managing FireWall-1 Using the Windows GUI* or *Managing FireWall-1 Using the OpenLook GUI*.



## FTP

The FTP Security Server provides Content Security based on FTP commands (PUT/GET), file name restrictions, and CVP inspection for files.

For information on defining FTP resources, see Chapter 6, "Resources," of *Managing FireWall-1 Using the Windows GUI* or *Managing FireWall-1 Using the OpenLook GUI*.

## CVP Inspection

CVP inspection is an integral component of FireWall-1's Content Security feature, and considerably reduces the vulnerability of protected hosts. CVP inspection examines all files transferred for all protocols. CVP configuration (which files to inspect, how to handle invalid files) is available for all Resource definitions. All FireWall-1 auditing tools are available for logging and alerting when these files are encountered.

CVP inspection is implemented by Content Vectoring Servers. The interaction between FireWall-1 and the Content Vectoring Server is defined by Check Point's OPSEC (Open Platform for Secure Enterprise Connectivity) framework. This interaction is depicted in FIGURE 3-2 on page 129.

For more information about OPSEC integration within FireWall-1, see <http://www.checkpoint.com/opsec>. If you would like to download evaluation versions of OPSEC-certified products, see <http://www.opsec.com>.

## Implementing CVP Inspection

In order to implement CVP inspection, proceed as follows:

- 1 Define a CVP Server.
- 2 Define Resource objects that specify CVP checking for the relevant protocols.
- 3 Define rules in the Rule Base that specify the action taken on connections that invoke each Resource.

### Defining a CVP Server

Content Vectoring Servers are defined in the **CVP Server Properties** window (see "CVP Servers" on page 98 of *Managing FireWall-1 Using the Windows GUI* or "CVP Servers" on page 78 of *Managing FireWall-1 Using the OpenLook GUI*).

### Defining Resources

The following CVP inspection options are available for all Resource definitions.

- **None** - The file is not inspected.
- **Read Only** - The file is inspected by the CVP Server. If the CVP Server rejects the file, it is not retrieved.
- **Read/Write** - The file is inspected by the CVP Server. If the CVP Server detects that the file is invalid (perhaps because it contains a virus), the CVP Server corrects the file before returning it to the Inspection Module.



## CVP Inspection

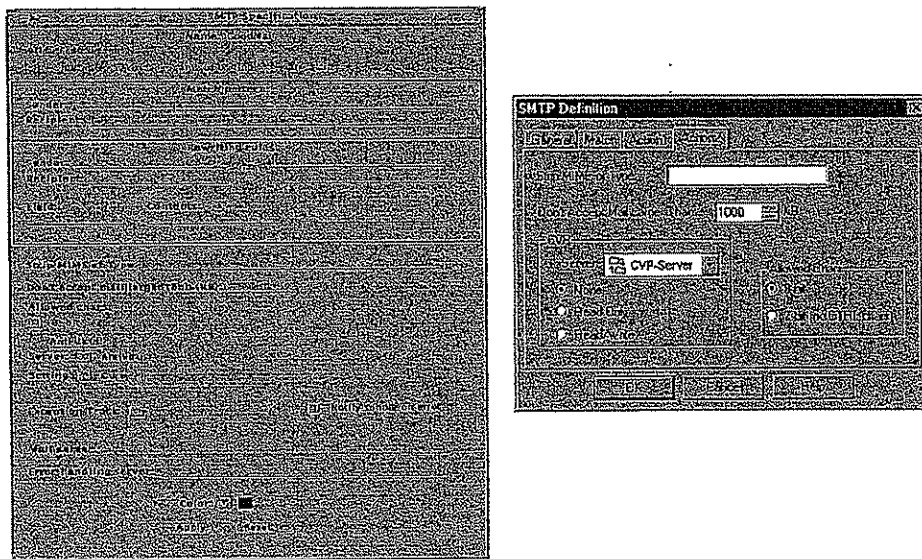


FIGURE 3-6 SMTP Resource with CVP properties (OpenLook and Windows)

### Defining Rules

Rules that specify CVP inspection do not replace rules that allow FTP, HTTP, or SMTP connections. Since FireWall-1 examines the Rule Base sequentially, you must define rules in the appropriate order to prevent unwanted traffic from entering your network.

Resource rules which accept HTTP, SMTP, and FTP connections must be placed before other rules which accept these services. If you define a rule that allows all HTTP connections before a rule which specifies CVP inspection on a URI Resource, you may be allowing unwanted traffic.

Similarly, CVP rules must be placed after rules which reject FTP, HTTP or SMTP Resource connections. For example, a rule rejecting large e-mail messages must come before a CVP rule allowing specific SMTP connections.

CHAPTER **4**

# Account Management

## In This Chapter

<i>Overview</i>	<i>page 135</i>
<i>Account Management Configuration</i>	<i>page 137</i>
<i>Proprietary Attributes</i>	<i>page 144</i>
<i>LDAP Properties</i>	<i>page 150</i>
<i>Configuring an LDAP Server for FireWall-1</i>	<i>page 152</i>
<i>Troubleshooting</i>	<i>page 154</i>

## Overview

The FireWall-1 Account Management system enables the Security Manager to integrate FireWall-1 with LDAP Servers, allowing user data to be shared between FireWall-1 and other applications.

The LDAP Servers and FireWall-1 can reside on different hosts and be maintained by different people. Separating the functionality of the two systems provides the following benefits:

- The system administrator can use existing LDAP-compliant databases without the need to import user data into FireWall-1.
- A single FireWall-1 system can be used by several departments or customers, each of which can manage its own users independently using a separate management client.
- Users can maintain and change their own passwords.
- There is no limit to the number of users that can be defined.

An additional feature is the live template. In the FireWall-1 user management model, changes made to a user template do not affect users previously defined using that template. In contrast, in the FireWall-1 Account Management system, changes made to a live template immediately apply to all users linked to the template.

## Overview

Users wishing to continue using the proprietary FireWall-1 user database may do so. Groups defined in both systems can be freely mixed in the Rule Base.

## The LDAP Model

LDAP (Lightweight Directory Access Protocol) is a lightweight version of the X.500 directory access protocol. LDAP is based on a Client/Server model in which an LDAP Client makes a TCP connection to an LDAP server, over which it sends requests and receives responses.

The LDAP information model is based on the entry, which contains information about some object (for example, a person). Entries are composed of attributes, which have a type and one or more values. The schema lists the attributes, their data types (for example, ASCII text, a JPEG photograph, etc.) and how those values behave during directory operations (for example, whether case is significant in comparisons).

Entries are organized in a tree structure, usually based on political, geographical, and organizational boundaries. Each entry is uniquely named relative to its sibling entries by its RDN (relative distinguished name) consisting of one or more distinguished attribute values from the entry. For example, the entry for the person Babs Jensen might be named with the "Barbara Jensen" value from the commonName attribute.

A globally unique name for an entry, called a DN (distinguished name), is constructed by concatenating the sequence of RDNs from the root of the tree down to the entry. For example, if Babs worked for the University of Michigan, the DN of her University of Michigan entry might contain:

```
"cn=Barbara Jensen, o=University of Michigan, c=US"
```

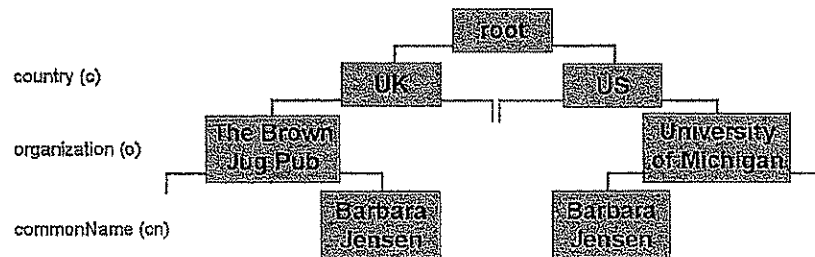
A DN is expressed in the "bottom up" sequence, that is, starting at the lowest level and moving up to the root of the tree.

A different Barbara Jensen who works at The Brown Jug Pub in London, England might have a DN of:

```
"cn=Barbara Jensen, o=The Brown Jug Pub, c=UK"
```

LDAP Servers

This is illustrated in FIGURE 4-1.



**FIGURE 4-1** LDAP Tree Example

LDAP provides operations to authenticate, search for and retrieve information, modify information, and add and delete entries from the tree.

### LDAP Servers

The LDAP information model is most appropriate for directory services, that is, information which is read much more frequently than it is modified. An LDAP Server makes the data in an LDAP-compliant directory available to LDAP Clients.

An LDAP directory can be indexed, which improves performance at the cost of the directory taking up more disk space.

### LDAP Schema

An LDAP schema is a description of the structure of the data in an LDAP directory.

## Account Management Configuration

### Account Management Components

The Account Management system comprises four components:

- 1 Firewall-1 Management Module (Version 4.0 and higher)
- 2 Firewall-1 Firewall Module (Version 4.0 and higher)
- 3 Check Point Account Management Client (AM Client)

The AM Client can be run from within the Firewall-1 GUI or as an independent stand-alone application. As a stand-alone application, it does not require that the Firewall-1 GUI be installed on the same machine as the AM Client.

The AM Client is described in *Check Point Account Management Client*.

## Account Management Configuration

## 4 LDAP Server (any LDAP Version 2.0 or higher compliant third-party server)

The LDAP server must be accessible to both the AM Client and to the FireWall Module, that is, both when a Security Policy is defined and when it is enforced.

## A Typical Configuration

A typical configuration is depicted in FIGURE 4-2.

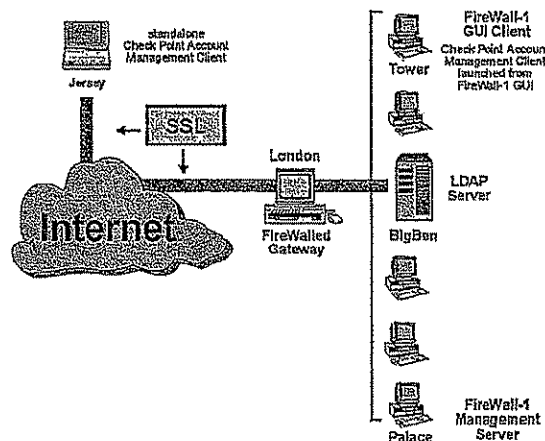


FIGURE 4-2 A typical Account Management configuration

Palace, the FireWall-1 Management Server, is the repository of the FireWall-1 database, which includes users defined with the proprietary FireWall-1 User Manager.

Palace's FireWall-1 GUI Clients, for example Tower, can define two kinds of users:

- FireWall-1 users — users defined in the FireWall-1 User Manager, using the FireWall-1 GUI and stored in the FireWall-1 proprietary database
- LDAP users — users defined on BigBen, the LDAP server, using the AM Client

These users can be shared between FireWall-1 and other network applications.

Jersey, on which FireWall-1 is not installed, can update only LDAP users, using the AM Client. In the configuration depicted in FIGURE 4-2, this communication channel is secured with SSL (Secure Socket Layer).

A system administrator can define a Security Policy on Palace, using the GUI Client on Tower, and define rules that specify FireWall-1 groups and LDAP groups. When the Security Policy is installed on the FireWalled gateway (London), the User Database (proprietary information about FireWall-1 users) is downloaded to London.

## Account Units

When a FireWall-1 user (a user defined in the FireWall-1 proprietary database) logs on to London, London has immediate access to the required authentication information in the FireWall-1 User Database. In contrast, when an LDAP user (a user defined in an LDAP Server) logs on and must be authenticated, London must communicate with the LDAP Server to obtain the required information.

In addition to maintaining LDAP users with the FireWall-1 Account Management Client and LDAP Server, it is possible to maintain LDAP users using any LDAP Version 2.0 and higher compatible server.

## Account Units

An LDAP Server can contain multiple branches ("o=University of Michigan,c=US", for example, is a branch). An LDAP Server and a subset of its branches constitute a FireWall-1 Account Unit. It is possible to maintain the LDAP user database using more than one Account Unit. The advantages of using more than one Account Unit are:

- *compartmentalization* — A large number of users can be distributed across several LDAP servers which may be partitioned into several Account Units, each of which is managed by a different administrator (see FIGURE 4-3 on page 139). In this way, both efficiency and security can be enhanced.
- *high availability* — Information can be duplicated on several servers. Some LDAP servers provide automatic tools for synchronizing servers.
- *remote sites* — It may be efficient to provide each geographically remote FireWall Module with a close at hand LDAP server.

FIGURE 4-3 depicts a configuration with four Account Units (two of them on the same LDAP server), each of which is managed from a different client.

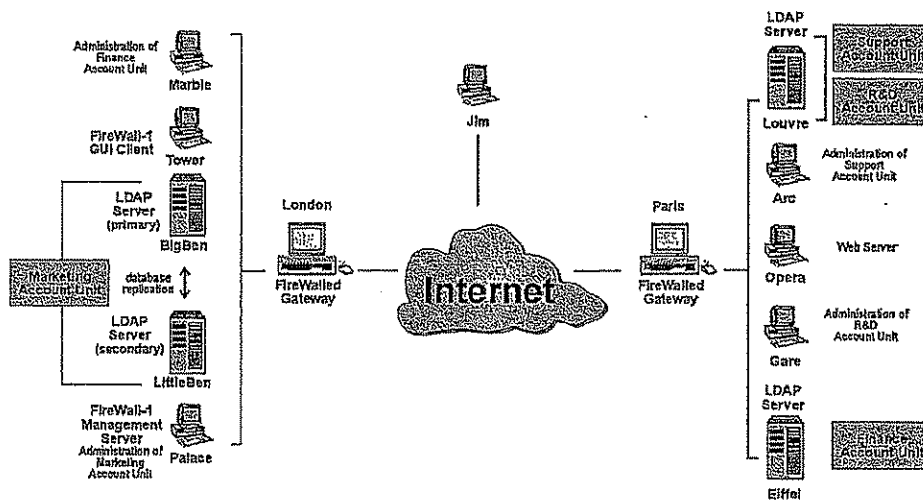


FIGURE 4-3 Multiple Account Units - Example Configuration

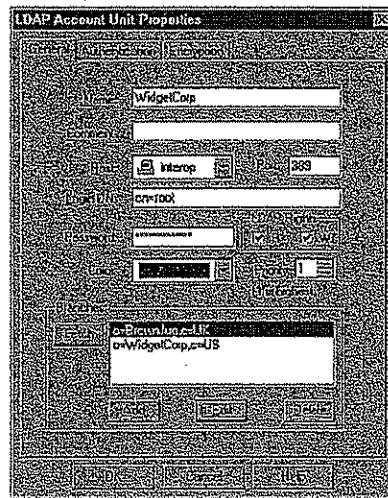


## Account Management Configuration

## Defining a Security Policy

To define a Security Policy that references users defined in an LDAP Account Unit, proceed as follows (in FireWall-1):

- 1 Define the LDAP properties in the **LDAP** tab of the **Properties Setup** window (see “LDAP Properties” on page 150).
- 2 Define the LDAP Server as a network object.  
  
See Chapter 2, “Network Objects” of *Managing FireWall-1 Using the Windows GUI* for information on how to define network objects.
- 3 Define an LDAP Account Unit in the **LDAP Account Unit Properties** window (FIGURE 4-4 on page 140).



**FIGURE 4-4** LDAP Account Unit Properties window — General tab

For information on defining Account Units, see Chapter 5, "Server Objects," of *Managing FireWall-1 Using the Windows GUI*.

## Enforcing a Security Policy

- 4 Define an external user group in the **External User Group (LDAP)** window (FIGURE 4-5).

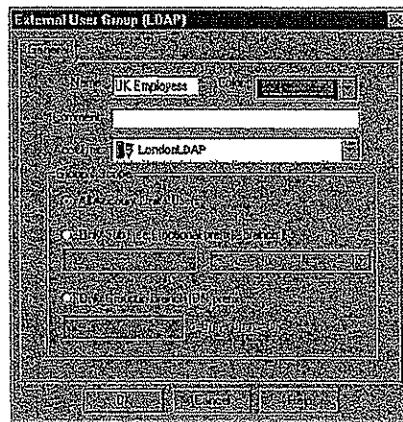


FIGURE 4-5 External User Group (LDAP) window

For information on defining external user groups, see "External Users and Groups" on page 74 of *Managing FireWall-1 Using the Windows GUI*.

- 5 Use the external group in a rule.

As illustrated in FIGURE 4-6, external groups are used in a Rule Base in exactly the same way as ordinary FireWall-1 groups are used.

No.	Source	Destination	Service	Action	Track	Install On
1	UK Employees@UKNet	Any	http	accept	Shot	Gateways
2	Any	Any	Any	deny	None	Gateways

FIGURE 4-6 External User Group in a Rule Base

For information on using groups in a rule, see Chapter 9, "Rule Base Management," of *Managing FireWall-1 Using the Windows GUI*.

## Enforcing a Security Policy

This section describes what happens when a user attempts to establish a connection through a FireWall Module when the Security Policy specifies groups defined on Account Units. The network configuration is depicted in FIGURE 4-7 on page 142.

## Account Management Configuration

Suppose user Jim attempts to connect to Opera, one of the computers protected by the FireWalled gateway Paris.

- 1 Paris scans its Rule Base and determines that the relevant rule is an authentication rule.

- 2 Paris asks Jim to identify himself (user name).

Jim can enter his login name or his full LDAP Distinguished Name, for example, "cn=Jim Smith,o=WidgetCorp,c=US".

- 3 Paris searches its FireWall-1 User Database for user Jim.

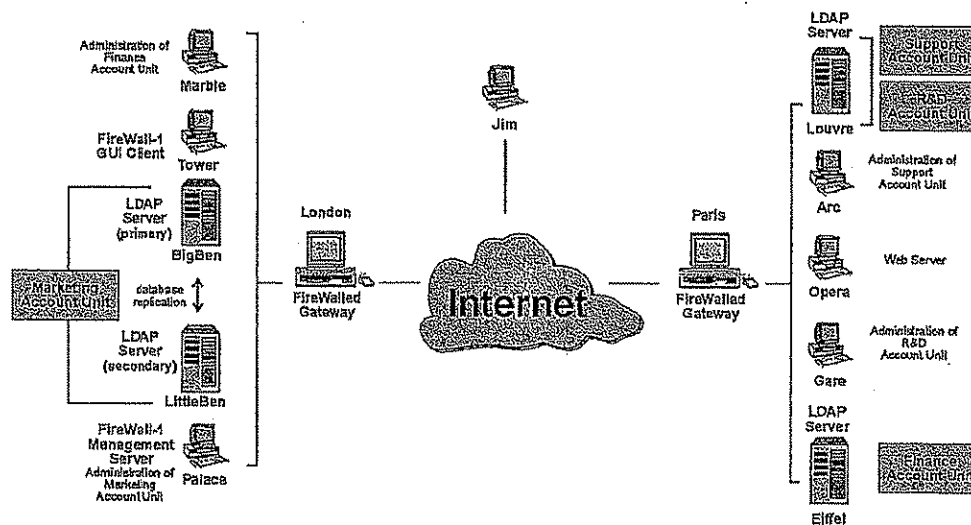


FIGURE 4-7 Enforcing a Security Policy

- 4 If Jim is found in the FireWall-1 User Database, then Paris authenticates Jim according to the attributes (authentication scheme, password *etc.*) defined in Jim's **User Properties** window (in the FireWall-1 GUI).



**Note** – The FireWall-1 User Database always has priority over Account Units. It is recommended that you define network and system administrators as FireWall-1 users, so that they will always be able to log in to the FireWall, even if the LDAP connection is down.

The other parameters (**Allowed Source**, **Allowed Destination**, **Time** *etc.*) must also be applicable. If Jim authenticates himself correctly, the connection is allowed; otherwise it is refused. In either case, the scenario ends at this point.

## Enforcing a Security Policy

- 5 If Jim is *not* found in the FireWall-1 User Database, then Paris queries all its Account Units, asking if any of them knows about Jim.
- 6 The query process terminates when any one of the following conditions is true:
  - All Account Units have replied.
  - The timeout period (see "LDAP Properties" on page 150) has elapsed.
  - The user was found in the highest priority Account Unit (see "LDAP Account Unit Properties Window — General Tab" on page 103 of *Managing FireWall-1 Using the Windows GUI*).
  - The user was found in an Account Unit *and* all Account Units with higher priorities have already replied that they do not know about the user.
- 7 If the user was not found in any Account Unit, then the authentication fails.
- 8 If the user was found, then Paris chooses the first user named Jim received from the Account Unit with the highest priority and ignores the other Account Units (if any). Suppose this is BigBen.



**Note** – If there is more than one user with the same name in an Account Unit, the first one is chosen and any others are ignored. If the **Display user's DN at login** property is enabled in the **LDAP** tab of the **Properties Setup** window (FIGURE 4-8 on page 150), you can verify that the correct entry is being used.

- 9 Paris queries BigBen to determine the groups to which Jim belongs.
- 10 Paris queries BigBen to determine Jim's template and applies the template values to Jim (if Jim is defined to inherit his values from a template).
- 11 Paris confirms the authentication scheme.

Jim's authentication scheme (as defined in the **Authentication** tab of his **User Properties** window in the Account Management Client GUI) must be:

- one of those allowed in the **Authentication** tab of BigBen's **LDAP Account Unit** window, *and*
- one of those selected in the **Authentication** tab of Paris' **Workstation Properties** window

If either of these conditions is not met, the connection is refused and the scenario ends.

- 12 Paris authenticates Jim according to his authentication scheme.

If Jim authenticates himself correctly, the connection is allowed; otherwise it is refused.

## LDAP Schema

The FireWall-1 LDAP schema is in `$FWDIR\lib\ldap\schema.ldif`.

## LDAP Schema

**Proprietary Attributes****OID**

Each of the proprietary object class and attributes (all of which begin with "fw1") have also a proprietary Object Identifier (OID), listed below.

**TABLE 4-1** Object Class OIDs

object class	OID
fw1template	1.3.114.7.3.2.0.1
fw1person	1.3.114.7.3.2.0.2

The OIDs for the proprietary attributes begin with the same prefix ("1.3.114.7.4.2.0.X"). Only the value of "X" is different for each attribute. The value for "X" is given in the table below.

## Proprietary Attributes

## Attributes

TABLE 4-2 Attributes

attribute	uid in OID	fw1person	fw1template	default	remarks
cn					The entry's name. In the Account Management Client, this is referred to as "Common Name". For users this can be different from the uid attribute — the name used to login to the FireWall. This attribute is also used to build the LDAP entry's distinguished name, that is, it is the RDN of the DN.
uid					The user's login name, that is, the name used to login to the Firewall Module. This attribute is passed to the external authentication system in all authentication methods except for "Internal Password", and must be defined for all these authentication schemes. The login name is used by FireWall-1 to search the LDAP server(s). For this reason, each user entry should have its own unique uid value. It is also possible to login to the firewall using the full DN. The DN can be used when there is an ambiguity with this attribute or in "Internal Password" when this attribute may be missing. The DN can also be used when the same user (with the same uid) is defined in more than one Account Unit on different LDAP Servers.
description				"no value"	Descriptive text about the user.
mail				"no value"	User's email address.
member					An entry can have zero or more values for this attribute. In a template: The DN of user entries using this template. DNs that are not users (object classes that are not one of: "person", "organizationalPerson", "inetOrgPerson" or "fw1person") are ignored. In a group: The DN of user, group or live template entries that are members of this group.



# **EXHIBIT 3**

## **PART 3**

## LDAP Schema

TABLE 4-2 Attributes (continued)

attribute	"X" in OID	fw1person	fw1template	default	remarks
userPassword					<p>Must be given if the authentication method (fw1auth-method) is "Internal Password". The value can be hashed using "crypt". In this case the syntax of this attribute is: "{crypt}xxxxxxxxxxxx", where:</p> <ul style="list-style-type: none"> <li>■ "xx" is the "salt"</li> <li>■ "xxxxxxxxxxxx" is the hashed password</li> </ul> <p>It is possible (but not recommended) to store the password without hashing. However, if hashing is specified in the LDAP Server, you should not specify hashing here, in order to prevent the password from being hashed twice. You should also use SSL in this case, to prevent sending an unencrypted password.</p> <p>The FireWall Module never reads this attribute, though it does write it. Instead, the LDAP bind operation is used to verify a password.</p>
fw1auth-method	1	✓	✓	"undefined"	<p>One of the following:</p> <ul style="list-style-type: none"> <li>■ "S/Key"                      ■ "RADIUS"</li> <li>■ "SecurID"                    ■ "TACACS"</li> <li>■ "OS Password"              ■ "Defender"</li> <li>■ "Internal Password"        ■ "undefined"</li> </ul> <p>This default value for this attribute is overridden by <b>Default Scheme</b> in the <b>Authentication</b> tab of the <b>Account Unit</b> window in the FireWall-1 GUI (see "LDAP Account Unit Properties Window — Authentication Tab" on page 105 of <i>Managing FireWall-1 Using the Windows GUI</i>).</p> <p>For example: an LDAP server can contain LDAP entries that are all of the object-class "person" even though the proprietary object-class "fw1person" was not added to the server's schema. If <b>Default Scheme</b> in the FireWall-1 GUI is "Internal Password", all the users will be authenticated using the password stored in the "userPassword" attribute.</p>

Proprietary Attributes

TABLE 4-2 Attributes (continued)

attribute	"x" in OID	fw1person	fw1template	default	remarks								
fw1auth-server	2	✓	✓		<p>The name of the server that will perform the authentication. This field must be given if fw1auth-method is "S/Key" or "RADIUS" or "TACACS". For all other values of fw1auth-method, it is ignored. Its meaning is given below:</p> <table><tr><th>method</th><th>meaning</th></tr><tr><td>S/Key</td><td>name of the workstation on which the FireWall Module is installed</td></tr><tr><td>RADIUS</td><td>name of a RADIUS server, a group of RADIUS servers, or "Any"</td></tr><tr><td>TACACS</td><td>name of a TACACS server</td></tr></table>	method	meaning	S/Key	name of the workstation on which the FireWall Module is installed	RADIUS	name of a RADIUS server, a group of RADIUS servers, or "Any"	TACACS	name of a TACACS server
method	meaning												
S/Key	name of the workstation on which the FireWall Module is installed												
RADIUS	name of a RADIUS server, a group of RADIUS servers, or "Any"												
TACACS	name of a TACACS server												
fw1pwdLastMod	3	✓	✓	If no value is given, then the password has never been modified.	The date on which the password was last modified. The format is <i>yyyymmdd</i> (for example, 20 August 1968 is 19680820). A password can be modified using the Account Management Client (see "New User Window - Authentication Tab" on page 47 of <i>Account Management Client</i> ), or through the FireWall Module as a part of the authentication process.								
fw1Skey-number	4	✓	✓		Length of initial S-Key chain. This attribute is required if the authentication method is S/Key.								
fw1Skey-seed	5	✓	✓		The seed from which the S-Key chain was generated (with the addition of a secret). This attribute is required if the authentication method is S/Key.								
fw1Skey-passwd	6	✓	✓		The last value of the initial S-Key chain. This attribute is required if the authentication method is S/Key.								
fw1Skey-mdm	7	✓	✓	MD4	The hash function used by S/Key. Valid values are "MD4" and "MD5". This attribute is required if the authentication method is S/Key.								

## LDAP Schema

TABLE 4-2 Attributes (continued)

attribute	"X" in OID	fw1person	fw1template	default	remarks
fw1expiration-date	8	✓	✓	"no value"	The last date on which the user can login to a Firewall Module, or "no value" if there is no expiration date. The format is yyyyymmdd (for example, 20 August 1968 is 19680820). The default is "no value".
fw1hour-range-from	9	✓	✓	"00:00"	The time from which the user can login to a Firewall Module. The format is hh:mm (for example, 8:15 AM is 08:15).
fw1hour-range-to	10	✓	✓	"23:59"	The time until which the user can login to a Firewall Module. The format is hh:mm (for example, 8:15 AM is 08:15).
fw1day	11	✓	✓	all days of the week	The days on which which the user can login to a Firewall Module. Can have the values "SUN", "MON", ... .
fw1allowed-src	12	✓	✓	"no value"	The names of one or more network objects from which the user can run a client, or "Any" to remove this limitation, or "no value" if there is no such client. The names should match the name of network objects defined in FireWall-1 management station.
fw1allowed-dst	13	✓	✓	"no value"	The names of one or more network objects which the user can access, or "Any" to remove this limitation, or "no value" if there is no such network object. The names should match the name of network objects defined in FireWall-1 management station.
fw1allowed-vlan	14	✓	✓	"no value"	currently not used
fw1SR-keym	15	✓	✓	"Any"	The algorithm used to encrypt the session key in SecuRemote. Can be "CLEAR", "FWZ1", "DES" or "Any".
fw1SR-datam	16	✓	✓	"Any"	The algorithm used to encrypt the data in SecuRemote. Can be "CLEAR", "FWZ1", "DES" or "Any".
fw1SR-mdm	17	✓	✓	"none"	The algorithm used to sign the data in SecuRemote. Can be "none" or "MD5".
fw1enc-fwz-expiration	18	✓	✓		The number of minutes after which a SecuRemote user must re-authenticate himself or herself to the FireWall.

Proprietary Attributes

TABLE 4-2 Attributes (continued)

attribute	"X" in OID	fw1person	fw1template	default	remarks
fw1sr-auth-track	19	✓	✓	"none"	The exception to generate on successful authentication via SecuRemote. Can be "none", "cryptlog" or "cryptalert".
fw1groupTemplate	20	✓	✓	"FALSE"	This flag is used to resolve a problem related to group membership. The group membership of a user is stored in the group entries to which it belongs and not in the user entry itself. Therefore there is no clear indication in the user entry if information from the template about group relationship should be used. If this flag is "TRUE", then the user is taken to be a member of all the groups to which the template is a member. This is in addition to all the groups in which the user is directly a member.
fw1ISAKMP-EncMethod	21	✓	✓	"DES", "3DES"	The key encryption methods for SecuRemote users using ISAKMP. This can be one or more of: "DES", "3DES". A user using ISAKMP may have both methods defined.
fw1ISAKMP-AuthMethods	22	✓	✓	"signatures"	The allowed authentication methods for SecuRemote users using ISAKMP. This can be one or more of: "preshared", "signatures".
fw1ISAKMP-HashMethods	23	✓	✓	"MD5", "SHA1"	The data integrity method for SecuRemote users using ISAKMP. This can be one or more of: "MD5", "SHA1". A user using ISAKMP must have both methods defined.
fw1ISAKMP-Transform	24	✓	✓	"ESP"	The IPSec Transform method for SecuRemote users using ISAKMP. This can be one of: "AH", "ESP".
fw1ISAKMP-DataIntegrityMethod	25	✓	✓	"SHA1"	The data integrity method for SecuRemote users using ISAKMP. This can be one of: "MD5", "SHA1".
fw1ISAKMP-SharedSecret	26	✓	✓		The pre-shared secret for SecuRemote users using ISAKMP.
fw1ISAKMP-DataEncMethod	27	✓	✓	"DES"	The data encryption method for SecuRemote users using ISAKMP.
fw1enc-Methods	28	✓	✓	"FWZ"	The encryption method allowed for SecuRemote users. This can be one or more of: "FWZ", "ISAKMP".

LDAP Properties

## LDAP Properties

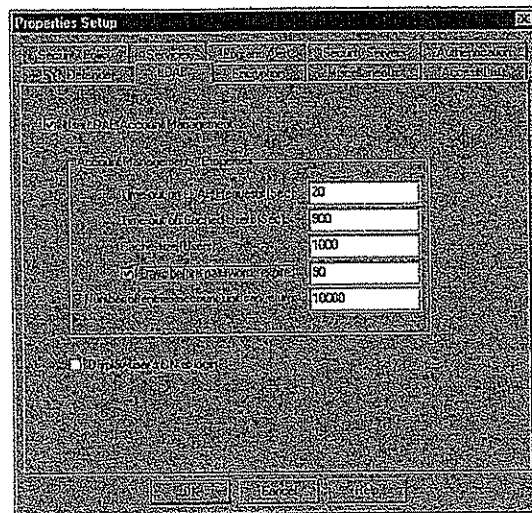



FIGURE 4-8 Properties Setup window — LDAP tab

To display the **Properties** window, click on  in the toolbar or select **Properties** from the **Policy** menu.

**Use LDAP Account Management** — Check this field if User Authentication will use LDAP Account Units, in addition to the FireWall internal User Database.

- If this field is checked, the other fields in the window are enabled.
- If this field is not checked, User Authentication will use only the FireWall internal User Database.

**Time-out on LDAP Requests** — An LDAP request will be considered to have timed out after this period (specified in seconds).

**Time-out on Cached Users** — A cached user will be considered to be out-of-date after this period (specified in seconds), and will be fetched again from the LDAP Server.

**Cache Size (Users)** — This field specifies the number of users that will be cached.

The cache is FIFO (first-in, first-out). When a new user is added to a full cache, the first user is deleted to make room for the new user. FireWall-1 does not query the LDAP Server for users already in the cache, unless the cache has timed out.



## Proprietary Attributes

**Days before Password Expires (0 = never)** — The number of days for which a user's password is valid.

This field is enabled when the checkbox is checked. If the field is not enabled, the user's password never times out.

After this period has passed, the user must define a *new* password. This is not to be confused with the case when the user is asked to re-authenticate after an FWZ SecuRemote connection has been open for a certain period of time. The re-authentication period is defined in the **FWZ Encryption** window (see "FWZ Properties" on page 60 of *Virtual Private Networking with FireWall-1*).



**Note** – This field does not apply ISAKMP pre-shared secrets and certificates, which do not expire.

If a user's password is modified using a tool other than the FireWall-1 Account Management Client, fw1pwdLastMod attribute is not updated, and the new password will expire on the day the old one would have expired.

For example, suppose that for user Alice, **Days before Password Expires** is 15. On January 1<sup>st</sup>, Alice modifies her password using the Check Point Account Management Client. fw1pwdLastMod is set to January 1<sup>st</sup>, so her password will expire on January 16<sup>th</sup>.

Suppose that on January 10<sup>th</sup>, Alice modifies her password again.

- If she uses the Check Point Account Management Client to modify her password, then:
  - fw1pwdLastMod is changed to January 10<sup>th</sup>.
  - Her new password is valid for 15 days from January 10<sup>th</sup>, and will expire on January 26<sup>th</sup>.
- If she uses a different LDAP Client to modify her password, then:
  - fw1pwdLastMod is not changed, and is still January 1<sup>st</sup>.
  - Her new password is valid for 15 days from January 1<sup>st</sup>, and will expire on January 16<sup>th</sup>.

When an user defined on an LDAP Account Unit enters a password, FireWall-1 checks whether the password has expired. If the password has expired, the user is prompted to enter a new password. The new password must be different from the old one, and must also satisfy the following conditions :

- minimum length
- minimum number of lowercase letters (a-z)
- minimum number of uppercase letters (A-Z)
- minimum number of symbols (non-letters and non-numbers)
- minimum number of digits (0-9)

## Configuring an LDAP Server for FireWall-1

The default values for these conditions are given in the `objects.C` file by the following parameters (the default setting is in parenthesis):

```
:props (
:passwd_min_length (0)
:passwd_min_num_of_lowercase (0)
:passwd_min_num_of_uppercase (0)
:passwd_min_num_of_symbols (0)
:passwd_min_num_of_numbers (0)
```

**Number of Users AU Can Return** — This field specifies the number of users that the Account Unit may return in response to a single query.

**Display user's DN at login** — If checked, then when an LDAP user logs in, his or her DN will be displayed before he or she is prompted for a password.

This property is a useful diagnostic tool when there is more than one user with the same name in an Account Unit. In this case, the first one is chosen and any others are ignored. If this property is enabled, the user can verify that the correct entry is being used.



**Note** — A user can log in either with a user name or with a DN.

## Exporting Users from the FireWall-1 User Database

You can export users from the FireWall-1 internal user database to an LDAP directory by using the `fw dbexport` command with the `-l` parameter. This command exports users or groups to an LDAP format file readable by most LDAP Servers.

For information about the `fw dbexport` command, see "Exporting a User Database" on page 288.

## Configuring an LDAP Server for FireWall-1

### LDAP Version

FireWall-1 is LDAP Version 2.0 compliant. The only Version 3.0 feature that FireWall-1 uses is the implementation of the **Fetch** button in the **General** tab of the **Account Unit Properties** window and in the Check Point Account Management Client (see "Branches" on page 104 of *Managing FireWall-1 Using the Windows GUI*).

Indexing

## Indexing

To maximize an LDAP Server's performance, it's recommended to index the LDAP Server according to the following attributes:

- DN
- UID
- member
- objectclass

These indexes reduce lookup time, but there is a trade-off between faster lookup times and the extra disk space needed to store the additional indexes.

## Schema Checking

When schema checking is enabled, LDAP requires that every object class and its associated attributes be defined in the directory schema.

When you first begin to use FireWall-1 Account Management, you should disable schema checking. Later, after you have entered the FireWall-1 object classes and attributes to the LDAP Server's schema, you can enable schema checking.

## Security Issues

### Access Control

You should set the following parameters on the LDAP Server to the specified values:

- default access — none
- username and password for FireWall — read/write access to branches containing FireWall-1 users

### FireWall-1 - LDAP Server Communication

There are three alternatives for securing communication between a FireWall Module or an Account Management Client and an LDAP Server:

- 1 If the LDAP Server is SSL-enabled, the FireWall Module and the Account Management Client can use SSL to communicate with the LDAP Server.
- 2 Use a VPN (Virtual Private Network) for the communication.
- 3 Put the LDAP Server inside a network protected by FireWall-1.

## Troubleshooting

### Damage Control

- 13** You can limit security exposure by not allowing the LDAP Server to authenticate users, and specifying only third-party authentication schemes (TACACS, RADIUS, AXENT) implemented on other machines.



**Note** – The FireWall-1 User Database always has priority over Account Units. It is recommended that you define network and system administrators as FireWall-1 users, so that they will always be able to log in to the FireWall, even if the LDAP connection is down.

## Troubleshooting

### FireWall-1 rejects the user's password

This might happen if the user is defined differently in the FireWall-1 user database, or in an Account Unit with a higher priority.

Check the **Display user's DN at login** field in the LDAP tab of the **Properties Setup** window (FIGURE 4-8 on page 150) and try again. The user's DN will be displayed, and you will know from where FireWall-1 is getting the user's password.

### User not found

Make sure that **Use LDAP Account Management** in the LDAP tab of the **Properties Setup** window (FIGURE 4-8 on page 150) is checked.

Using the Account Management Client, verify that the user is indeed defined on the Account Unit.

### Changes made in the Account Management Client do not affect FireWall-1

Changes take effect only after one of the following happens:

- the cache times out (see FIGURE 4-8 on page 150)
- the Security Policy is installed
- the User Database is downloaded (see "Database Installation" on page 79 of *Managing FireWall-1 Using the Windows GUI*)

CHAPTER **5**

# Network Address Translation

## In This Chapter

<i>Introduction</i>	<i>page 155</i>
<i>Translation Modes</i>	<i>page 158</i>
<i>Address Translation and Routing</i>	<i>page 165</i>
<i>IANA Recommendations</i>	<i>page 170</i>
<i>Supported Services</i>	<i>page 170</i>
<i>Generating Address Translation Rules Automatically</i>	<i>page 171</i>
<i>Configuring Address Translation — Windows GUI</i>	<i>page 173</i>
<i>Configuring Address Translation — Command Line Interface</i>	<i>page 189</i>
<i>Address Translation Examples</i>	<i>page 191</i>
<i>Managing PIX Address Translation</i>	<i>page 199</i>
<i>Advanced Topics</i>	<i>page 205</i>
<i>Frequently Asked Questions</i>	<i>page 210</i>

## Introduction

### The Need for Address Translation

The need for IP address translation — replacing one IP address in a packet by another IP address — arises in two cases:

- 1 The network administrator wishes to conceal the network's internal IP addresses from the Internet.

The administrator may reason that there is nothing to be gained, from a security point of view, by making a network's internal addresses public knowledge.

## Introduction

- 2 An internal network's IP addresses are invalid Internet addresses (that is, as far as the Internet is concerned, these addresses belong to another network).

This situation may have arisen for historical reasons: an internal network was originally not connected to the Internet and its IP addresses were chosen without regard to Internet conventions. If such a network is then connected to the Internet, its long-established internal IP addresses cannot be used externally. Changing these addresses may be impractical or unfeasible.

In both cases, the internal IP addresses cannot be used on the Internet. However, Internet access must still be provided for the internal hosts with the invalid or secret IP addresses.

Application gateways (proxies) have historically served as a partial solution to these problems. For example, to hide his or her internal IP addresses, a user can TELNET to a gateway and from there continue to the Internet through a proxy. FireWall-1 can be easily set up to provide and enforce such a scheme for a wide variety of services (FTP, TELNET, HTTP, and almost all other TCP, UDP and RPC services). Moreover, FireWall-1 supplements this scheme by providing user authentication on the gateway.

On the other hand, proxies do have drawbacks:

- Proxies are tailored per application, so it is impossible to use applications that are not proxied, inbound or outbound.
- Proxies are not transparent, so that even authorized outbound users need to go through the application on the gateway, and impose a large overhead on the gateway host. Once a connection is accepted by a proxy, it functions as a packet forwarder at the application layer, which is an inefficient use of resources.
- It is difficult to provide good proxies for protocols other than TCP.

In contrast, FireWall-1's generic and transparent fully RFC 1631 compliant Address Translation feature provides a complete and efficient solution. The administrator can determine which internal addresses are to be concealed (that is, mapped to the FireWalled host's IP address) and which are to be mapped to a range of IP addresses visible to the Internet. At the same time, internal hosts can be configured to be accessible from the Internet even though their internal IP addresses are invalid Internet addresses. FireWall-1 achieves full Internet connectivity for internal clients at the maximum bandwidth possible through a standard workstation.

Address Translation can be used to implement "one way routing," so that there is no route from the outside to an internal network or to hosts.



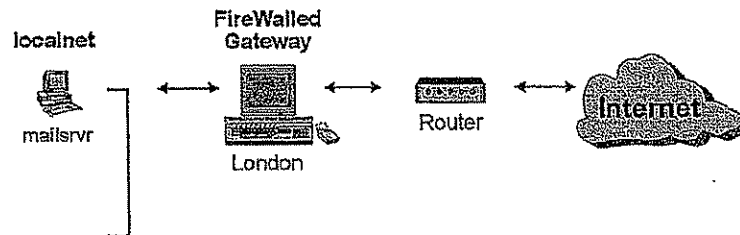
**Note** – Address Translation changes IP addresses in the packet, so it is almost always necessary to make some changes in the routing tables to ensure that packets with translated addresses reach their proper destinations.



Example

**Example**

Consider the following network configuration:



**FIGURE 5-1** Example Network Configuration

Suppose the administrator of this network wishes to provide mail services to the internal (private) hosts, but the internal IP addresses cannot be used, for one of the reasons stated above (see "The Need for Address Translation" on page 155.)



**Note** – The gateway has a valid IP address which cannot be concealed.

One possible solution is to move the mail server (which is currently on one of the internal hosts) to the gateway. This solution is not optimal, because of:

- the significant overhead the mail server imposes on the gateway
- reduced security
- the administrative overhead incurred when modifying the configuration

A better solution might be to implement Address Translation on the gateway, as follows, using the Static Destination Mode of Address Translation (see "Static Destination Mode" on page 164):

- The mail server is assigned a valid IP address (its public IP address), which is exposed to the Internet. However, internally, the mail server retains its existing (private) IP address.
- Incoming mail arrives at the gateway, where the destination IP address (the mail server's public IP address) is translated to its private address. The source IP address of outgoing mail is translated from the mail server's private IP address to its public IP address.

Routing tables on the gateway and router may have to be modified to implement this scheme (see "Address Translation and Routing" on page 165).

## Translation Modes

**Configuring Address Translation**

There are three methods of configuring Address Translation:

**Automatic Configuration** — Address Translation is configured as a property of a machine, network or Address Range.

This is the recommended method. Under this method, rules for an Address Translation Rule Base are automatically generated, and the object's properties are applied whenever the object is used in the Security Policy. In addition, numerous implementation details are automatically handled correctly (for example, Anti-Spoofing). If you use one of the other methods, you must account for these implementation details manually.

Automatic configuration is the simplest method to use, but it is somewhat inflexible: the generated rules cannot be modified, but you can add rules (with the second method — see below) before and after the automatically generated rules.

For information on this method, see "Generating Address Translation Rules Automatically" on page 171.

**Address Translation Rules** — The System Administrator defines an Address Translation Rule Base, in many ways similar to a Security Policy Rule Base.

This method is available only under the FireWall-1 Windows GUI (Windows and X/Motif only). You can also add Address Translation rules before and after the rules generated automatically by the previous method, but you cannot modify or delete the automatically generated rules.

This method is more difficult to use than the previous method, but is more powerful and more flexible.

For information on this method, see "Configuring Address Translation — Windows GUI" on page 173.

**Command Line Interface** — The System Administrator defines Address Translation rules using a command line interface application (fwxl.conf), or directly edits the text file \$FWDIR/conf/xlate.conf.

In earlier versions of FireWall-1, this was the only available method, but its use is no longer recommended.

For information on this method, see "Configuring Address Translation — Command Line Interface" on page 189.

**Translation Modes**

FireWall-1 supports two kinds of Address Translation:

**Dynamic (Hide)** — Many invalid addresses are translated to a single valid address, and dynamically assigned port numbers are used to distinguish between the invalid addresses.

## Hide Mode

Dynamic Address Translation is called Hide Mode, because the invalid addresses are "hidden" behind the valid address. For details of this mode, see "Hide Mode" on page 159.

**Static** — Each invalid address is translated to a corresponding valid address.

There are two modes of Static Address Translation:

- Static Source Mode (see "Static Source Mode" on page 162)
- Static Destination Mode (see "Static Destination Mode" on page 164)

### In This Section

<i>Hide Mode</i>	<i>page 159</i>
<i>Static Source Mode</i>	<i>page 162</i>
<i>Static Destination Mode</i>	<i>page 164</i>

### Hide Mode

Hide Mode is used for connections initiated by hosts in an internal network, where the hosts' IP addresses are invalid. In Hide Mode, the invalid internal addresses are hidden behind a single valid external address, using dynamically assigned port numbers to distinguish between them.



**Note** – The IP address of a gateway's external interface must never be hidden.

### Assigning Port Numbers

Port numbers are dynamically assigned from two pools of numbers:

- from 600 to 1023
- from 10,000 to 60,000

If the original port number is less than 1024, then a port number is assigned from the first pool. If the original port number is greater than 1024, then a port number is assigned from the second pool. FireWall-1 keeps track of the port numbers assigned, so that the original port number is correctly restored for return packets. A port number currently in use is not assigned again to a new connection.

### Limitations

Hide Mode has several limitations:

- Hide Mode allows no access initiated from the outside to the "hidden" hosts, that is, an external machine cannot connect to any of the hosts whose addresses have been translated. For example, in the configuration in FIGURE 5-3 on

### Translation Modes

page 161, if you run your HTTP server on 200.0.0.108 (one of the internal machines with an invalid address), external machines will not be able to connect to your HTTP server using 199.203.145.35 (the gateway's valid address) as the destination.

This limitation can also be considered an advantage of Hide Mode.

- Hide Mode cannot be used for protocols where the port number cannot be changed.
- Hide Mode cannot be used when the external server must distinguish between clients on the basis of their IP addresses, since all clients share the same IP address under Hide Mode.

### Example

Suppose localnet is an internal network with invalid addresses are as follows:

Valid IP address	Invalid IP addresses
199.203.145.35	200.0.0.100 - 200.0.0.200

199.203.145.35 is the address of gateway's external interface.

You can hide the invalid addresses behind the valid address by specifying Address Translation in the **Address Translation** tab of localnet's **Network Properties** window as follows:

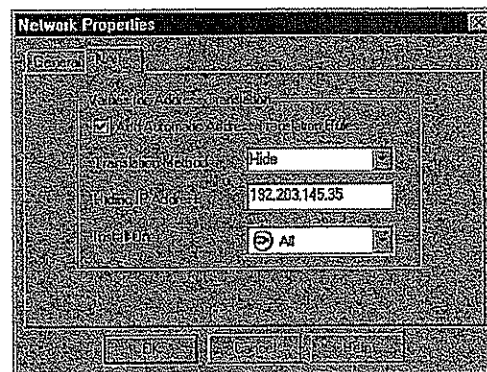


FIGURE 5-2 Address Translation tab for localnet

Hide Mode

Source addresses of outbound packets from hosts in localnet will be translated to 199.203.145.35, as illustrated in FIGURE 5-3. The source port number serves to direct reply packets to the correct host.

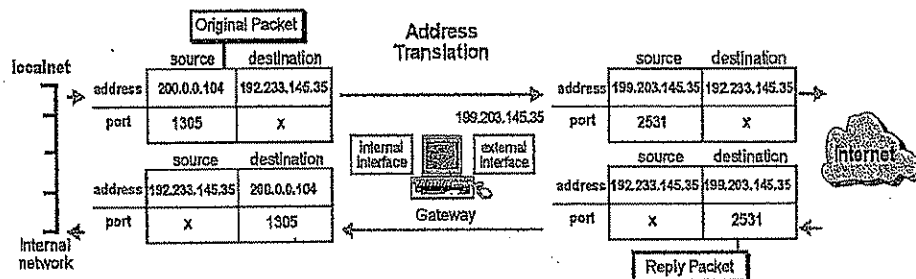


FIGURE 5-3 Hide Mode Address Translation

The following two Address Translation rules (FIGURE 5-4) are automatically generated from the above definition (FIGURE 5-2 on page 160):

No.	Original Packet			Translated Packet			Install On
	Source	Destination	Service	Source	Destination	Service	
1	localnet	localnet	Any	= Original	= Original	= Original	All
2	localnet	Any	Any	localnet (Hiding Address)	= Original	= Original	All

FIGURE 5-4 Hide Mode Automatically Generated Rules

The first rule (which does not translate anything) applies to connections from the gateway to localnet and prevents the address of the gateway's internal interface from being translated<sup>1</sup>.

The second rule expresses the Address Translation defined in the Address Translation tab (FIGURE 5-2 on page 160) and illustrated in FIGURE 5-3. Note the small letter H under localnet's icon, which indicates Hide Mode translation.

For a detailed description of the meaning of the fields in an Address Translation Rule Base, see "Structure of an Address Translation Rule" on page 173.



**Note** – Routing tables on the gateway and router may have to be modified to implement this scheme (see "Address Translation and Routing" on page 165).

<sup>1</sup> For an explanation of why this rule is necessary, see "Can I translate the gateway's internal address?" on page 211.

## Translation Modes

**Choosing the Valid External Address for Hide Mode**

You can choose to hide the internal IP addresses either behind the IP address of the gateway's external interface, or behind an imaginary IP address.

If you hide the internal IP addresses behind the IP address of the gateway's external interface ...

You will not have to make any changes to your routing tables (see "Address Translation and Routing" on page 165), because presumably the routing tables are already correctly configured for the gateway's external interface.

On the other hand, you may have problems when a hidden connection shadows a connection originating on the gateway itself. For example, suppose a user on the gateway TELNETs to an external server, and is allocated the local TCP port 10001 by the gateway's TCP module. Next, a user on one of the internal hosts also TELNETs to the external-server and, because the connection is hidden, it is allocated the same TCP port 10001 by the FireWall Module on the gateway. In this event, packets returning from the external TELNET server to the first TELNET client will be (incorrectly) diverted to the internal host, where they will be ignored.

If you hide the internal IP addresses behind an imaginary IP address ...

You will probably have to change the routing tables (see "Address Translation and Routing" on page 165) so that replies to the imaginary IP address are directed to the gateway, but you will not have problems with shadowed connections as described above.

**Statically Translating Addresses****Static Source Mode**

Static Source Mode translates invalid internal IP addresses to valid IP addresses, and is used when the connection is initiated by internal clients with invalid IP addresses. Static Source Mode ensures that the originating hosts have unique, specific valid IP addresses, and is usually used together with Static Destination Mode.

When you generate Address Translation rules automatically, Static Source Mode and Static Destination Mode rules are always generated in pairs.

**Example**

Suppose localnet is an internal network with invalid addresses, but a corresponding set of valid addresses is available, as follows:

Valid IP addresses	Invalid IP addresses
199.203.73.15 - 199.203.73.115	200.0.0.100 - 200.0.0.200



## Statically Translating Addresses

You can translate the invalid addresses to the valid addresses by specifying Address Translation in the Address Translation tab of localnet's **Workstation Properties** window as follows:

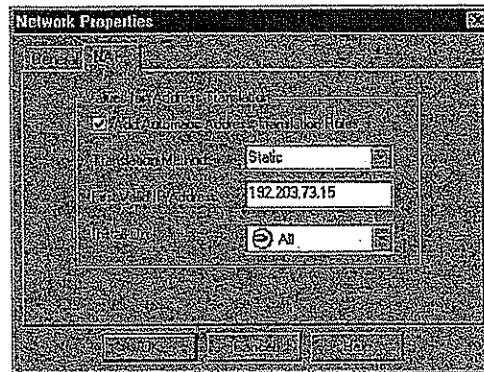


FIGURE 5-5 Static Address Translation

The invalid addresses of hosts in localnet will be translated to the valid addresses starting at 199.203.73.15.

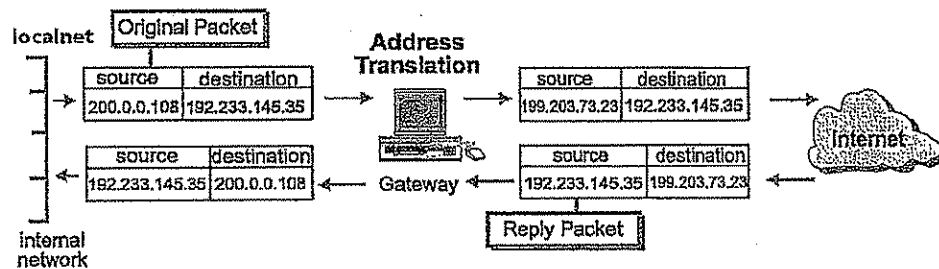


FIGURE 5-6 Address Translation using Static Source Mode

### Translation Modes

The following three Address Translation rules (FIGURE 5-7) are automatically generated from the above definition (FIGURE 5-5 on page 163):

No.	Original Packet			Translated Packet			Install On
	Source	Destination	Service	Source	Destination	Service	
1	Any	localnet	Any	Original	Original	Original	All
2	localnet	Any	Any	localnet (Valid Addresses)	Original	Original	All
3	Any	localnet (Valid Addresses)	Any	Original	localnet	Original	All

**FIGURE 5-7** Automatically Generated Address Translation rules for Static Translation

The first rule (which does not translate anything) applies to connections from the gateway to localnet and prevents the address of the gateway's internal interface from being translated<sup>1</sup>.

Note that two static translation rules are generated:

- The first static translation rule (rule number 2) is a Static Source Mode rule, and expresses the Address Translation illustrated in FIGURE 5-6.
- The second static translation rule (rule number 3) is the corresponding Static Destination rule and expresses the Address Translation illustrated in FIGURE 5-8 on page 165 (see "Static Destination Mode" on page 164).

For a detailed description of the meaning of the fields in an Address Translation Rule Base, see "Structure of an Address Translation Rule" on page 173.



**Note** – Routing tables on the gateway and router may have to be modified to implement this scheme (see "Address Translation and Routing" on page 165).

### Static Destination Mode

Static Destination Mode translates valid addresses to invalid addresses for connections initiated by external clients. Static Destination Mode is used when servers inside the internal network have invalid IP addresses, and ensures that packets entering the internal network arrive at their proper destinations. Static Destination Mode is usually used together with Static Source Mode.

When you generate Address Translation rules automatically, Static Source Mode and Static Destination Mode rules are always generated in pairs.

<sup>1</sup> For an explanation of why this rule is necessary, see "Can I translate the gateway's internal address?" on page 211.

## Configuring Routing on the Gateway

**Example**

Suppose localnet is an internal network with invalid addresses, but a corresponding set of valid addresses is available, as follows:

Valid IP addresses	Invalid IP addresses
199.203.73.15 – 199.203.73.115	200.0.0.100 – 200.0.0.200

The second static translation rule (rule number 3) in FIGURE 5-7 on page 164 (generated from the **Address Translation** tab in FIGURE 5-5 on page 163) translates the valid addresses starting at 199.203.73.15 to the corresponding invalid addresses starting at 200.0.0.100. This is illustrated in FIGURE 5-8.

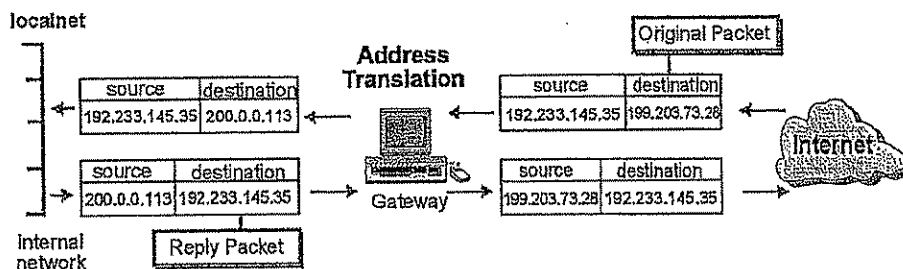


FIGURE 5-8 Address Translation using Static Destination Mode



**Note** – Routing tables on the gateway and router may have to be modified to implement this scheme (see “Address Translation and Routing” below).

## Address Translation and Routing

### Configuring Routing on the Gateway

To correctly implement Address Translation, you must ensure that a return packet intended for a host whose address has been translated is routed back to that host. There are two routing issues involved:

- ensuring that the packet reaches the gateway
- ensuring that the gateway forwards the packet to the correct interface and host



**Note** – You will usually have to reconfigure your routing tables on the gateway (and on any intervening routers) to implement Address Translation.

## Address Translation and Routing

**Ensuring That the Packet Reaches the Gateway****From the Inside**

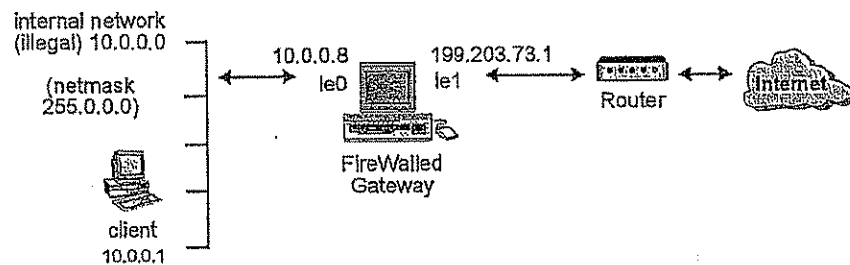
The internal hosts (whose addresses are being translated) need a default route to the gateway, just as they do without Address Translation.

**From the Outside**

The translated (valid) addresses must be published, so that replies will be routed back to the gateway.

However, a router positioned between the gateway and the Internet may fail to route reply packets to the translating gateway. Instead, the router rather sends ARP requests, looking for the physical (MAC) address of the imaginary translated address.

For example, consider the following network configuration (FIGURE 5-9), where the internal network's invalid addresses are hidden behind the non-existent IP address 199.203.73.3 (FIGURE 5-10 on page 167):



**FIGURE 5-9** Hiding a Network

When the client (10.0.0.1) initiates a connection to the outside world, the gateway translates the packet's source address to 199.203.73.3, so when a reply packet arrives from the server, its destination address is 199.203.73.3. If no static route exists, the router sees that the packet is destined for a directly attached network

## Configuring Routing on the Gateway

(199.203.73.x) and sends an ARP request querying for the physical address (MAC) of 199.203.73.3. But since 199.203.73.3 is an imaginary address, the router receives no response for its query and drops the packet.

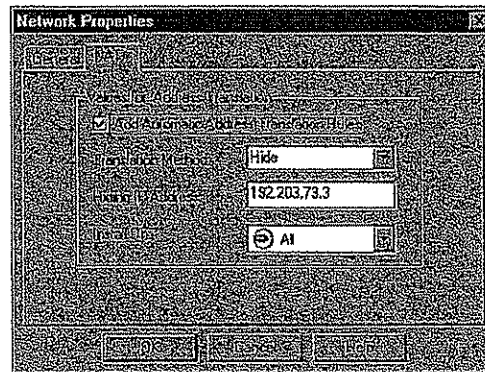


FIGURE 5-10 Hiding a Network Behind a Non-Existent IP Address

There are three ways to solve this problem:

1 Reconfigure the Address Translation.

Hide the invalid network behind the gateway's external address, as follows:

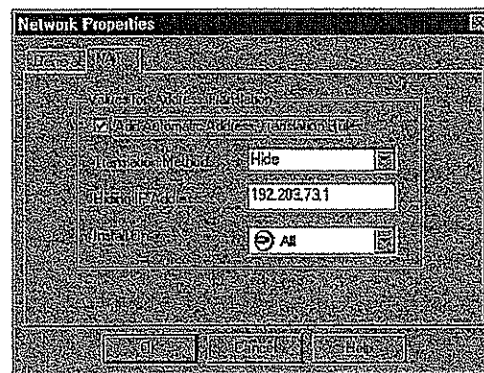


FIGURE 5-11 Hiding a Network Behind a Real IP Address



## Address Translation and Routing

- 2** Another way of solving the problem is to change the routing on the router.

Define a static route on the router, using the equivalent of the Unix command:

```
route add 199.203.73.3 199.203.73.1 1
```

The route command can be added to the FireWall-1 startup script (\$FWDIR/bin/fwstart) so that it is automatically executed each time FireWall-1 is started.

- 3** A third way of solving the problem is to change the routing on the gateway (proxy ARP method).

**Unix** — On the gateway, link 199.203.73.3 to the MAC address of the gateway's external interface.

```
arp -s 199.203.73.3 <MAC Address> pub
```

**NT** — Create a text file named local.arp in the \$FWDIR\state directory. Each line in the file should be of the form:

```
<MAC Address> <IP Address>
```

where <MAC Address> is 199.203.73.3's MAC Address, and  
<IP Address> is the gateway's external interface.

### Ensuring That the Gateway Forwards the Packet to the Correct Host

When translating the destination address of a connection (Static Destination Mode), packets may be forwarded to the wrong gateway interface if there are no static routes on the gateway to the translated (new) destination.

In this case, Address Translation takes place in the gateway only after internal routing but before transmission (see "Address Translation and Anti-Spoofing" on page 205), so the gateway's routing sees an external destination address. To ensure that these packets are correctly routed to an internal host (and not bounced back out to the Internet), use static routing (the OS route command) to define the same "next hop" for both addresses.



## Configuring Routing on the Gateway

For example, consider the following configuration:

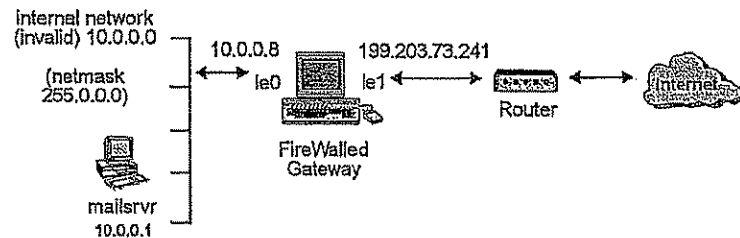


FIGURE 5-12 Static Address Translation

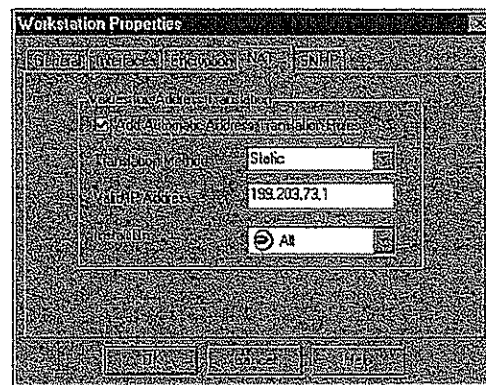


FIGURE 5-13 Static Address Translation for mailsrvr

This results in the rules below (FIGURE 5-16):

No.	Original Packet			Translated Packet			Install On
	Source	Destination	Service	Source	Destination	Service	
1	mailsrvr	Any	Any	mailsrvr (Valid Address)	Original	Original	All
2	Any	mailsrvr (Valid Address)	Any	Original	mailsrvr	Original	All

FIGURE 5-14 Static Address Translation rules

**IANA Recommendations**

The second rule will work correctly only if the gateway knows that in order to reach the address 199.203.73.1, it should forward the packet to 10.0.0.1. To make this happen, add a static route on the gateway, using the command:

```
route add 199.203.73.1 10.0.0.1 1
```

The router too has to know that the packets to the translated address must be routed through the gateway. This can be achieved either by defining a static route on the router, or by having the gateway publish (to the router) the fact it has a route to the translated address. For additional information about this problem, see "Ensuring That the Packet Reaches the Gateway" on page 166.

**IANA Recommendations**

RFC 1918 documents private address spaces for organizations that will not have hosts on the Internet.

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private networks:

**TABLE 5-1 Private Networks Address Space**

class	from IP address ...	to IP address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

An enterprise that decides to use IP addresses in the address spaces defined above can do so without any coordination with IANA or an Internet registry. The address space can thus be used by many enterprises. Addresses within this private address space will only be unique within the enterprise.

**Supported Services****New Services**

Network Address Translation now supports H.323, NetShow and VxTreme.

**Restrictions**

TABLE 5-2 lists restrictions that apply to Address Translation when used with protocols that carry IP addresses or port numbers in the packet's data portion, as opposed to the IP or TCP or UDP header.

FTP port command

TABLE 5-2 lists these restrictions.

**TABLE 5-2** Address Translation — Service Restrictions

Service	Restrictions
Xing	does not work with Address Translation
rshell	does not work with Address Translation
sglnet2	If the listener and server are on two different hosts whose IP addresses are being translated, then the difference between their untranslated IP addresses must be the same as the difference between their translated IP addresses. For example, if their original IP addresses are 200.200.200.1 and 200.200.200.11 (a difference of 10), then their translated IP addresses can be 199.199.199.20 and 199.199.199.30 (also a difference of 10), but not 199.199.199.20 and 199.199.199.40 (a difference of 20).

#### FTP port command

The FTP port command has been rewritten to support Address Translation, as specified in RFC 1631.

## Generating Address Translation Rules Automatically

### Overview

You can generate Address Translation rules for machines, networks and Address Ranges automatically, using the **Address Translation** tab of the network object's **Properties** window (Windows GUI) or the **Host Address Translation Properties** and **Network Address Translation Properties** windows (OpenLook GUI).

### Generating Address Translation Rules Automatically

For example, FIGURE 5-15 shows the **Address Translation** tab of the **Network Properties** window (Windows GUI) and the **Network Address Translation Props** window (OpenLook GUI).

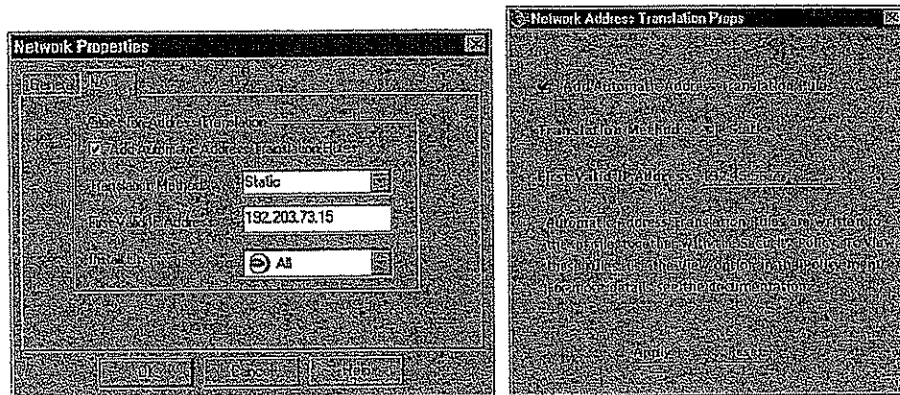


FIGURE 5-15 Automatic Address Translation for a Network

To generate Address Translation rules for a network object, proceed as follows:

- 1 Define the object whose address(es) will be translated using the Network Object Manager.

For information on the Network Object Manager, see Chapter 2, "Network Objects" of *Managing FireWall-1 Using the Windows GUI*.

- 2 In the **Address Translation** tab of the object's **Properties** window (Windows GUI) or the **Host Address Translation Properties** or **Network Address Translation Properties** windows (OpenLook GUI), check **Add Automatic Address Translation Rules**.

When this box is checked, the other fields in the window are enabled.

- 3 Select a **Translation Method** from the drop-down menu.

For information about translation methods, see "Translation Modes" on page 158.

- 4 Enter an IP address for the translation.

If the **Translation Method** is **Hide**, then the IP address is the one behind which the object's addresses will be hidden (see "Hide Mode" on page 159).

If the **Translation Method** is **Static**, then the IP address is the first one in the range to which the object's addresses will be translated (see "Statically Translating Addresses" on page 162).

## Overview

- 5 In **Install On**, select a FireWalled object on which to install the generated Address Translation rule.

All means all the FireWalled objects that are able to perform Address Translation.

- 6 Click on **OK** or on **Apply**.

To view the Address Translation Rule Base (including the automatically generated rules), select the **Address Translation** tab in the Rule Base Editor (Windows and X/Motif only) or examine the .pf file.

The automatically generated rules are colored differently from manually defined rules, and are positioned first in the Address Translation Rule Base. Automatically generated rules cannot be modified using the Rule Base Editor, nor can you change their sequence. The automatically generated rules themselves can only be modified by editing the fields in the **Address Translation** tabs.

However, you can add rules before and after the automatically generated rules (see "Configuring Address Translation — Windows GUI" on page 173). If you add rules before the automatically generated rules and then add more automatically generated rules, the new automatically generated rules will be positioned together with the other automatically generated rules.



**Note** — If a host for which Address Translation has been defined has more than one IP addresses (for example, if it is a gateway with multiple interfaces), the only IP address that will be translated is the IP address specified in the **General** tab of the **Workstation Properties** window (Windows GUI) or in the **Workstation Properties** window (OpenLook GUI).

## Configuring Address Translation — Windows GUI

### Overview

In the Windows GUI, Address Translation can be configured in the form of an Address Translation Rule Base. The Rule Base expression of an Address Translation rule enables you to:

- specify objects by name rather than by IP address
- restrict rules to specified destination IP addresses, as well as to the specified source IP Addresses
- translate both source and destination IP addresses in the same packet
- restrict rules to specified services (ports)
- translate ports

### Structure of an Address Translation Rule

An Address Translation rule, like a Security Policy rule, consists of two elements:

- conditions that specify when the rule is to be applied



## Configuring Address Translation — Windows GUI

- the action to be taken when the rule is applied (that is, when the conditions are satisfied)

In the Windows GUI (FIGURE 5-16), the Address Translation Editor is divided into four sections:

- **Original Packet**
- **Translated Packet**
- **Install On**
- **Comment**

No.	Original Packet			Translated Packet			Install On	Comment
	Source	Destination	Service	Source	Destination	Service		
1	Any	Any	Any	Original	Any	Any	AI	Automatic rule (see the network object data).
2	Any	mslsvr (Valid Address)	Any	Original	mslsvr	Original	AI	Automatic rule (see the network object data).

FIGURE 5-16 Address Translation Rules in the Windows GUI

Original Packet and Translated Packet consist of, in turn:

- **Source**
- **Destination**
- **Service**

Original Packet specifies the conditions, that is, when the rule is applied.

Translated Packet specifies the action to be taken when the rule is applied.

The action is always the same:

- translate **Source** under **Original Packet** to **Source** under **Translated Packet**
- translate **Destination** under **Original Packet** to **Destination** under **Translated Packet**
- translate **Service** under **Original Packet** to **Service** under **Translated Packet**

If an entry under **Translated Packet** is **Original**, then the corresponding entry under **Original Packet** is not translated. TABLE 5-3 presents the various possibilities, using **Service** as an example.

TABLE 5-3 Condition vs. Translation

Original Packet Service is ...	Translated Packet Service is ...	
	Original	<new service>
Any	no conditions on <b>Service</b> , and <b>Service</b> is not translated	invalid combination — Security Policy will not verify
<old service>	the rule applies only to packets whose <b>Service</b> is <old service>, and <b>Service</b> is not translated	the rule applies only to packets whose <b>Service</b> is <old service>, and <old service> is translated to <new service>



## Address Translation Rule Base Example

## Address Translation Rule Base Example

FIGURE 5-17 shows an example of an Address Translation Rule Base.

No.	Original Packet			Translated Packet			Install On	Comment
	Source	Destination	Service	Source	Destination	Service		
1	MyNetwork	*	*	*	*	*	DMZ	Hide Mode
2	IllegalAddresses	*	*	LegalAddresses	*	*	DMZ	Static Source
3	*	LegalAddresses	*	*	IllegalAddresses	*	DMZ	Static Destination
4	*	*	StandardPorts	*	DMZ-Servers	*	DMZ	Static Service

FIGURE 5-17 Manually Added Address Translation Rules

#### Rule 1

The first rule in FIGURE 5-17 (a Hide Mode rule — note the small letter H under natasha's icon) specifies that:

**Condition** — when the original packet's **Source** address belongs to the network object **MyNetwork**

**Action** — hide its **Source** address behind the address of the network object **natasha**

#### Rule 2

The second rule in FIGURE 5-17 (a Static Source Mode rule) specifies that:

**Condition** — when the original packet's **Source** address is in the address range **IllegalAddresses**

**Action** — translate its **Source** address to the corresponding address in the address range **LegalAddresses**

#### Rule 3

The third rule in FIGURE 5-17 (a Static Destination Mode rule) specifies that:

**Condition** — when the original packet's **Destination** address is in the address range **LegalAddresses**

**Action** — translate its **Destination** address to the corresponding address in the address range **IllegalAddresses**

#### Rule 4

The fourth rule in FIGURE 5-17 specifies that:

**Condition** — when the original packet's **Service** is in the service range **StandardPorts** and its **Destination** is **DMZ-Servers**

## Configuring Address Translation — Windows GUI

**Action** — translate its **Service** to the corresponding **Service** in the service range **NonStandardPorts**



**Note** – The first three rules in this example can be automatically generated by the method described in "Generating Address Translation Rules Automatically" on page 171. The last rule cannot be automatically generated.

### Compound Conditions

Conditions under **Original Packet** are ANDed together. For example, the fourth rule in FIGURE 5-17 has a compound condition, that is, there are two conditions to be met, both of which must be true in order for the rule to apply.

The two conditions are:

- 1 The original packet's service number is in the service range **StandardPorts**.
- 2 The original packet's **Destination** is **DMZ-Servers**.

It is not possible to express a compound condition in the command line representation.

### Multiple Translation

If the addresses in two internal networks are invalid, there may be problems in communications between the two networks (see "Gateway with Three Interfaces" on page 194 for further information), which arise because both the source and destination addresses of packets must be translated.

The Windows GUI allows the specification of multiple translations in a single rule. For example, FIGURE 5-18 shows a rule in which both the source and destination addresses of packets are translated.

No.	Original Packet			Translated Packet			Install On	Comment
	Source	Destination	Service	Source	Destination	Service		
1	10.10.10.10	10.10.10.10	80	10.10.10.10	10.10.10.10	80	GUI	

FIGURE 5-18 Multiple Translation rule

For a detailed example of when a rule like this is necessary, see "Gateway with Three Interfaces" on page 194.

### Defining Address Translation Rules

To define an Address Translation rule using the Windows GUI, you must first define the objects that will be used in the rule.

Under **Source** and **Destination**, you can use any Machine or Network network object, including groups and Address Range objects.

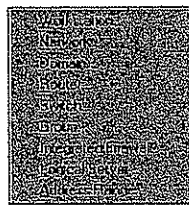
## Defining Address Translation Rules

Under **Service**, you can use any TCP or UDP **Services** object, including groups and **Port Range** objects.

### Address Range

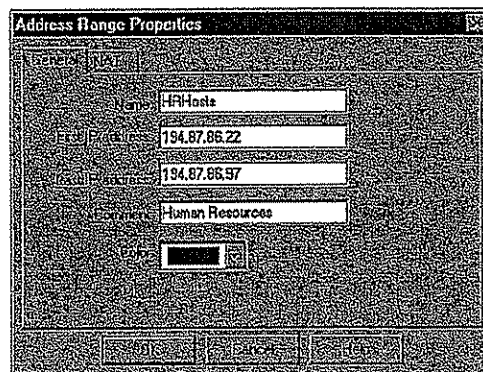
## Defining a Range of Addresses

To define a range of addresses, open the **Address Range Properties** window (FIGURE 5-20 on page 177) by selecting **Address Range** from the **Add Network Object** menu.



**FIGURE 5-19** Add Network Object menu

For information on how to display the **Add Network Object** menu, see “Defining Network Objects” on page 15 of *Managing FireWall-1 Using the Windows GUI*.



**FIGURE 5-20** Address Range Properties window

**Name** — the object's name

**First IP Address** — the first IP Address in the range

**Last IP Address** — the last IP Address in the range

## Configuring Address Translation — Windows GUI

**Comment** — descriptive text

This text is displayed on the bottom of the **Network Object** window when this item is selected.

**Color** — the color of the object's icon

Select the desired color from the drop-down list.

### Port Range

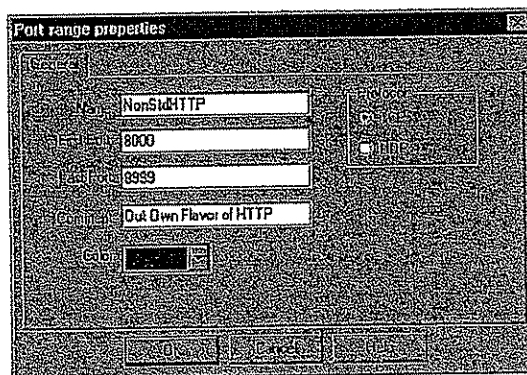
Defining a Range of Ports

To define a range of services, open the **Port Range Properties** window (FIGURE 5-22 on page 178) by selecting **Port Range** from the **Add Service Object** menu.



**FIGURE 5-21** Add Service Object menu

For information on how to display the **Add Service Object** menu, see “Defining Services” on page 81 of *Managing FireWall-1 Using the Windows GUI*.



**FIGURE 5-22** Port Range Properties window

**Name** — the object's name

**First Port** — the first service in the range

**Last Port** — the last service in the range

## Using the Address Translation Rules Editor

**Comment** — descriptive text

This text is displayed on the bottom of the **Network Object** window when this item is selected.

**Color** — the color of the object's icon

Select the desired color from the drop-down list.

**Protocol** — select TCP or UDP

## Using the Address Translation Rules Editor

To display the Address Translation Rules Editor (FIGURE 5-23), select the **Address Translation** tab in the Rule Base Editor.

No.	Original Packet			Translated Packet			Install On	Comment
	Source	Destination	Service	Source	Destination	Service		
1				1				
2				2				
3				3				
4				4				
5	hybridLocalNet	YasodCHZ	Any	Internet	hybridCHZ	Original	All	

FIGURE 5-23 Address Translation Rules Editor

To return to the Rule Base Editor, select the **Rule Base** tab.

An Address Translation Rule Base is part of a Security Policy. If you have more than one Security Policy, then each of them can have a corresponding Address Translation Rule Base. The Address Translation Rule Base is installed when the Security Policy is installed.







## Configuring Address Translation — Windows GUI

**Editing an Address Translation Rule Base****Adding a Rule**

You can add a rule at any point in the Address Translation Rule Base, except between automatically generated rules.

**TABLE 5-4** Adding a Rule

To add a rule	Select from menu	Toolbar Button
after the last rule	Rule, Add, Bottom	
before the first rule	Rule, Add, Top	
after the current rule	Rule, Add, Before	
before the current rule	Rule, Add, After	

A new rule will be added to the Address Translation Rule Base, and default values will appear in all the data fields. You can modify the default values as needed.



**Note** – To select a rule or rules, select their numbers.

**Modifying a Rule's Data Fields**

To modify a data field in a rule, right click on the value. A menu will be displayed, from which you can choose the new value.



## Using the Address Translation Rules Editor

## Original Packet — Source

**Source** can consist of only one object. The types of objects allowed for **Source** under **Original Packet** depend on what is specified for **Source** under **Translated Packet**, as listed in TABLE 5-5.

TABLE 5-5 Original Packet - Source

	If Translated Packet - Source is ...		
	Original	Hide	Static
<b>Original Packet - Source can be ...</b>	Machine, Network, Address Range or a group of one of these	Machine, Network, Address Range or a group of one of these	Machine, Network, Address Range but not a group

**Add** — The **Object Manager** window (FIGURE 5-24) is displayed, from which you can select a network object.

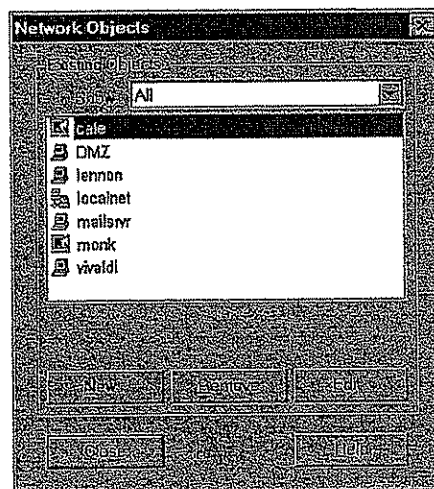


FIGURE 5-24 Object Manager window

**Replace** — The **Object Manager** window (FIGURE 5-24) is displayed, from which you can select an object to replace the object currently in the rule's **Source**.

**Edit** — Edit the object in the rule's **Source**.

The appropriate window is opened (depending on the type of the selected object), and you can change the object's properties.

**Delete** — Delete the object currently in the rule's **Source**.

**Cut** — Delete the object currently in the rule's **Source** and put it on the clipboard.

## Configuring Address Translation — Windows GUI

**Copy** — Copy the object currently in the rule's **Source** to the clipboard.

**Paste** — Paste the object on the clipboard in the rule's **Source**.

## Original Packet — Destination

**Destination** can consist of only one object. The types of objects allowed for **Destination** under **Original Packet** depend on what is specified for **Destination** under **Translated Packet**, as listed in .

TABLE 5-6 Original Packet - Destination

	If Translated Packet - Destination is ...		
	Original	Hide	Static
<b>Original Packet - Destination can be ...</b>	Machine, Network, Address Range or a group of one of these	Machine, Network; Address Range or a group of one of these	Machine, Network, Address Range but not a group

**Add** — The **Object Manager** window (FIGURE 5-24 on page 181) is displayed, from which you can select a network object.

**Replace** — The **Object Manager** window ( on page 181) is displayed, from which you can select an object to replace the object currently in the rule's **Destination**.

**Edit** — Edit the object in the rule's **Destination**.

The appropriate window is opened (depending on the type of the selected object), and you can change the object's properties.

**Delete** — Delete the object currently in the rule's **Destination**.

**Cut** — Delete the object currently in the rule's **Destination** and put it on the clipboard.

**Copy** — Copy the object currently in the rule's **Destination** to the clipboard.

**Paste** — Paste the object on the clipboard in the rule's **Destination**.

## Original Packet — Service

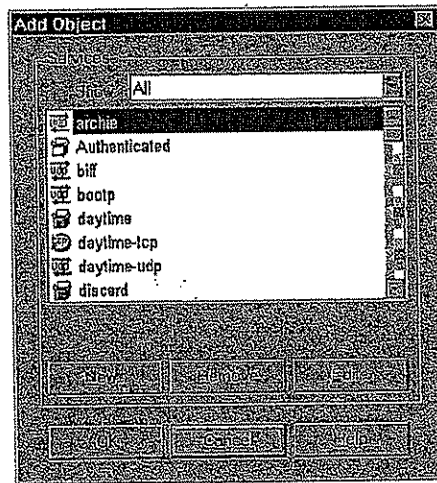
**Services** can consist of only one object. The types of objects allowed for **Services** under **Original Packet** depend on what is specified for **Services** under **Translated Packet**, as listed in TABLE 5-7.

TABLE 5-7 Original Packet - Services

	If Translated Packet - Services is ...		
	Original	Hide	Static
<b>Original Packet - Services can be ...</b>	TCP, UDP, Range or group of one of the above	TCP, UDP, Range or group of one of the above	TCP, UDP, Range but not a group

Using the Address Translation Rules Editor

**Add** — The Services window (FIGURE 5-25) is displayed, from which you can select a service.



**FIGURE 5-25** Services window

**Replace** — The Services window (FIGURE 5-25) is displayed, from which you can select an object to replace the object currently in the rule's Services.

**Edit** — Edit the service.

The appropriate window is opened (depending on the type of the selected service), and you can change the service's properties.

**Delete** — Delete the object currently in the rule's Services.

**Cut** — Delete the object currently in the rule's Services and put it on the clipboard.

**Copy** — Copy the object currently in the rule's Services to the clipboard.

**Paste** — Paste the object on the clipboard in the rule's Services.

## Configuring Address Translation — Windows GUI

## Translated Packet — Source

**Source** can consist of only one object. The types of objects allowed for **Source** depend on the type of Address Translation, as listed in .

TABLE 5-8 Translated Packet - Source

	If the Address Translation is	
	Hide	Static
Translated Packet - Source can be ...	Machine, Network, or Range of same size as <b>Original Packet - Source</b>	Machine, Network, Router, or Range of size 1

**Add (Static)** — The **Object Manager** window (FIGURE 5-24 on page 181) is displayed, from which you can select a network object.

The **Source** object under **Original Packet** will be translated to **Source** under **Translated Packet**, in **Source Static Mode**.

**Replace (Static)** — The **Object Manager** window (FIGURE 5-24 on page 181) is displayed, from which you can select an object to replace the object currently in the rule's **Source**.

**Replace (Static)** is only available when the **Source** object was added by **Add (Static)**. If you wish to replace an **Add (Hide)** object by an **Add (Static)** object, first delete the **Add (Hide)** object, and then choose **Add (Static)** from the menu.

**Add (Hide)** — The **Object Manager** window (FIGURE 5-24 on page 181) is displayed, from which you can select a network object.

The **Source** object under **Original Packet** will be translated to **Source** under **Translated Packet**, in **Hide mode**.

**Replace (Hide)** — The **Object Manager** window (FIGURE 5-24 on page 181) is displayed, from which you can select an object to replace the object currently in the rule's **Source**.

**Replace (Hide)** is only available when the **Source** object was added by **Add (Hide)**. If you wish to replace an **Add (Static)** object by an **Add (Hide)** object, first delete the **Add (Static)** object, and then choose **Add (Hide)** from the menu.

**Edit** — Edit the **Source** object.

The appropriate window is opened (depending on the type of the **Source** object), and you can change the object's properties.

**Delete** — Delete the object currently in the rule's **Source**.

After you delete the object, **Source** is set to **Original**.

**Cut** — Delete the object currently in the rule's **Source** and put it on the clipboard.

## Using the Address Translation Rules Editor

After you cut the object, **Source** is set to **Original**.

**Copy** — Copy the object currently in the rule's **Source** to the clipboard.

**Paste** — Paste the object on the clipboard in the rule's **Source**.

## Translated Packet — Destination

**Destination** can consist of only one object. The types of objects allowed for **Destination** depend on the type of Address Translation, as listed in TABLE 5-9.

TABLE 5-9 Translated Packet - Destination

	If the Address Translation is	
	Hide	Static
Translated Packet - Destination can be ...	Machine, Network, or Range of same size as Original Packet - Destination	Machine, Network, Router, or Range of size 1

**Add (Static)** — The **Object Manager** window (FIGURE 5-24 on page 181) is displayed, from which you can select a network object.

The **Destination** object under **Original Packet** will be translated to **Destination** under **Translated Packet**, in **Destination Static Mode**.

**Replace (Static)** — The **Object Manager** window (FIGURE 5-24 on page 181) is displayed, from which you can select an object to replace the object currently in the rule's **Destination**.

**Replace (Static)** is only available when the **Destination** object was added by **Add (Static)**.

**Edit** — Edit the **Destination** object.

The appropriate window is opened (depending on the type of the **Destination** object), and you can change the object's properties.

**Delete** — Delete the object currently in the rule's **Destination**.

After you delete the object, **Destination** is set to **Original**.

**Cut** — Delete the object currently in the rule's **Destination** and put it on the clipboard.

After you cut the object, **Destination** is set to **Original**.

**Copy** — Copy the object currently in the rule's **Destination** to the clipboard.

**Paste** — Paste the object on the clipboard in the rule's **Destination**.

## Configuring Address Translation — Windows GUI

## Translated Packet — Service

Service can consist of only one object. The types of objects allowed for **Service** are:

- TCP
- UDP
- Port Range

**Add (Static)** — The **Service** window (FIGURE 5-25 on page 183) is displayed, from which you can select a network object.

The **Service** object under **Original Packet** will be translated to **Service** under **Translated Packet**.

**Replace (Static)** — The **Service** window (FIGURE 5-25 on page 183) is displayed, from which you can select an object to replace the object currently in the rule's **Service**.

**Replace (Static)** is only available when the **Service** object was added by **Add (Static)**.

**Edit** — Edit the **Service** object.

The appropriate window is opened (depending on the type of the **Service** object), and you can change the object's properties.

**Delete** — Delete the object currently in the rule's **Service**.

After you delete the object, **Service** is set to **Original**.

**Cut** — Delete the object currently in the rule's **Service** and put it on the clipboard.

After you cut the object, **Service** is set to **Original**.

**Copy** — Copy the object currently in the rule's **Service** to the clipboard.

**Paste** — Paste the object on the clipboard in the rule's **Service**.

**Install On**




The **Install On** field specifies which FireWalled objects will enforce the rule. You cannot change the **Install On** field for automatically generated rules, but you can change it for manual rules.



## Using the Address Translation Rules Editor

To modify the **Install On** field, right click on it. A menu is displayed, from which you can select one of the values listed in TABLE 5-10.

TABLE 5-10 Install On Menu

Install On	Meaning
	<b>Gateways</b> — Enforce on all network objects defined as gateways.
	<b>Integrated FireWalls</b> — Enforce on all network objects defined as integrated FireWalls.
	<b>Targets</b> — Enforce on the specified target object(s) only.

If you choose **Targets**, then the **Select Target** window is displayed, from which you can choose a FireWalled gateway or host (but not a router), on which to install the Address Translation rule.

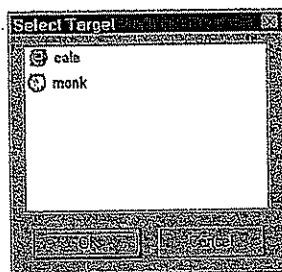


FIGURE 5-26 Select Target window

## Configuring Address Translation — Windows GUI

## Comment

You can add comments to a rule. Double click on the **Comment** field to open the **Comment** window (FIGURE 5-27).

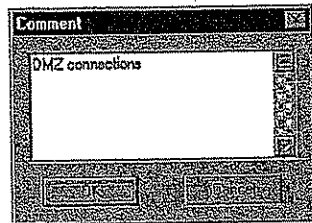





FIGURE 5-27 Comment window

Type any text you wish in the text box and click on **OK**.

## Copying, Cutting and Pasting Rules

To copy, cut or paste, select a rule or rules by selecting their numbers.

TABLE 5-11 Copying, Cutting and Pasting Rules

Action	Select from menu	Toolbar Button
Cut	Edit, Cut	
Copy	Edit, Copy	
Paste	Edit, Paste	

If you choose **Paste**, then the **Paste** menu will be opened. You must then select **Before**, **After**, **Top**, or **Bottom** to specify where in the Rule Base to paste the rule.

Using the Address Translation Rules Editor

## Configuring Address Translation — Command Line Interface

To configure Address Translation, run the Address Translation configuration utility `fwxl.conf`.

A listing of the current configuration is displayed, and then you are asked to select one of the following options:

```
Which of the following do you want ?
(1) Add/Change a translation entry
(2) Delete a translation entry
(3) Add interface
(4) Delete interface
(5) Add host
(6) Delete host
(7) Save configuration
(8) Restore configuration from Disk
(9) Quit
```

From this point on, you can modify the configuration or quit.

To restrict Address Translation to a subset of the gateway's interfaces, select the "Delete interface" and "Add Interface" options.

By default, Address Translation is installed on all FireWalled hosts, except for routers and embedded systems. You can install Address Translation on subset of the FireWalled hosts, select the "Delete host" and "Add host" options from the menu.

The Address Translation you have configured will be in effect starting with the next time you install a Security Policy, either by selecting **Install** from the **Policy** menu (in the Rule Base editor) or using the command line.

The Address Translation rules are in the file `$FWDIR/conf/xlate.conf`.

## Configuring Address Translation — Command Line Interface

**Differences Between the Command Line Interface and the GUI**

There are a number of significant differences between the Command Line and Rule Base expressions of Address Translation rules:

TABLE 5-12 Differences between Command Line and Rule Base expression

	GUI	command line
addresses	by name	by IP Address
range to range mapping	verifies that both ranges contain the same number of objects	only the first item in the range is specified
compound conditions	available	not available
multiple translation	available	not available
translated addresses expressed as	machines, networks, ranges, groups	only machines and machine ranges

For example, the first three rules in the Address Translation rules shown in FIGURE 5-17 on page 175 would be written as follows using the command line interface:

No.	From Original Address (Port)	To Original Address (Port)	Method	First Translated Address (Port)
0	172.45.126.1	172.45.126.39	FWXT_HIDE	172.45.125.60
1	192.9.200.9	192.9.200.9	FWXT_SRC_STATIC	172.45.125.209
2	172.45.125.209	172.45.125.209	FWXT_DST_STATIC	192.9.200.9

The fourth rule cannot be expressed in the command line interface (see "Multiple Translation" on page 176).



**Note** – If you previously used `fwx1conf` to configure your Address Translation rules, you must convert your configuration file (`$FWDIR/conf/xlate.conf`) to the format supported by the Windows GUI. If you did not do this when you upgraded your FireWall-1 software, you can convert the configuration file by running the FireWall-1 configuration program. For additional information, see Chapter 2, "Installing FireWall-1" in *Getting Started with FireWall-1*.

Gateway with Two Interfaces

## Address Translation Examples

<i>Gateway with Two Interfaces</i>	<i>page 191</i>
<i>Gateway with Three Interfaces</i>	<i>page 194</i>

### Gateway with Two Interfaces

Consider the following network and Address Translation configuration:

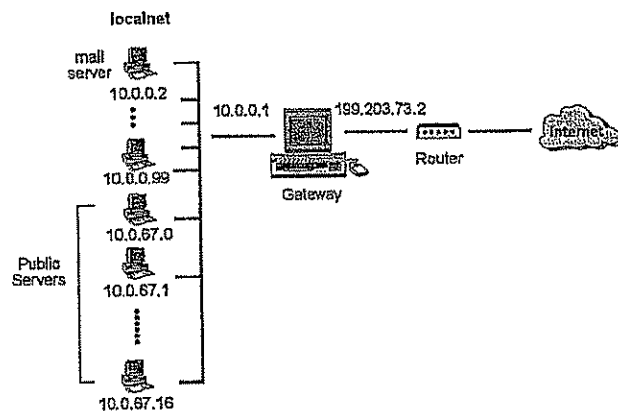


FIGURE 5-28 Gateway with Two Interfaces Example - Network

### Defining Address Translation

Since the mailserver accepts and initiates connections, it requires static translation, as shown in FIGURE 5-29 on page 192.

## Address Translation Examples

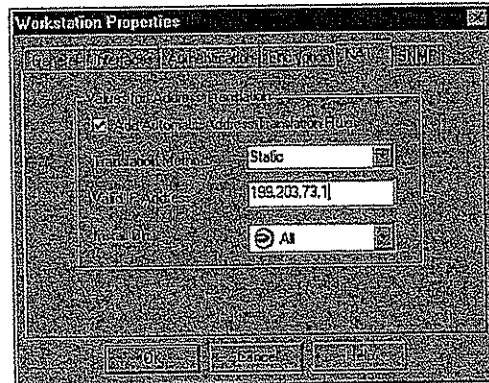


FIGURE 5-29 mailserver - static translation

Similarly, the Address Range from 10.0.67.0 to 10.0.67.16 is meant to provide public services, such as HTTP or FTP, to the outside world, and so it too requires Static Translation.

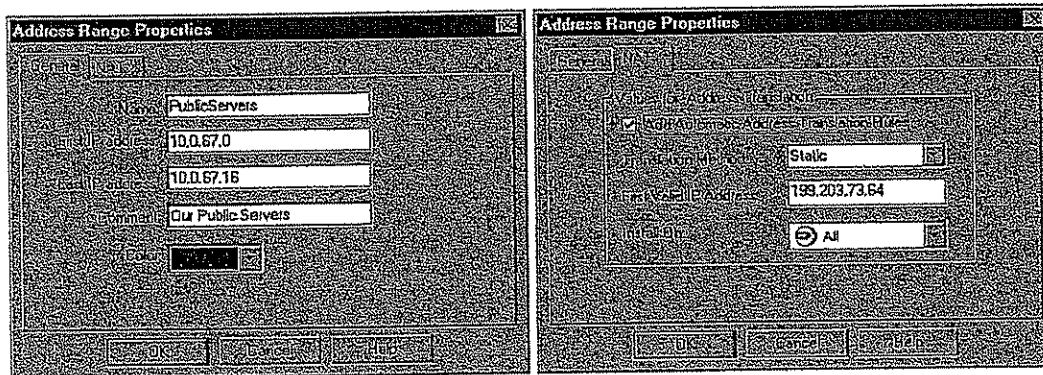


FIGURE 5-30 PublicServers Address Range

These addresses are mirrored as the seventeen (17) addresses from 199.203.73.64 to 199.203.73.80. So, for example, when an outside machine sends a packet to IP address 199.203.73.70, the packet will actually arrive at 10.0.67.6.



## Gateway with Two Interfaces

Finally, localnet addresses will be hidden behind the IP address of the gateway's external interface, 199.203.73.2 (FIGURE 5-31).

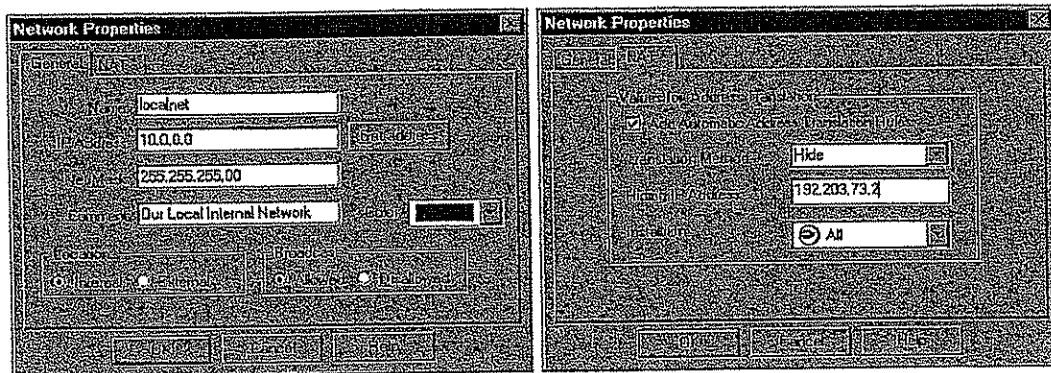


FIGURE 5-31 localnet Network Properties and Address Translation tabs

The rules generated from these definitions are shown in FIGURE 5-32.

No.	Original Packet			Translated Packet		
	Source	Destination	Service	Source	Destination	Service
1	mailserver	Any	Any	mailserver (Valid Address)	Original	Original
2	Any	mailserver (Valid Address)	Any	Original	mailserver	Original
3	PublicServers	PublicServers	Any	Original	Original	Original
4	PublicServers	Any	Any	PublicServers (Valid Addresses)	Original	Original
5	Any	PublicServers (Valid Addresses)	Any	Original	PublicServers	Original
6	localnet	localnet	Any	Original	Original	Original
7	localnet	Any	Any	localnet (Hiding Address)	Original	Original

FIGURE 5-32 Address Translation Rule Base

### Routing

Assume that the Internet routes IP addresses in the network 199.203.73.0 to the router.

Then you should ensure that:

- 1 The router routes IP addresses in the network 199.203.73.0 to the gateway.

## Address Translation Examples

- 2 The gateway routes IP address 199.203.73.3 to the internal interface (10.0.0.1).
- 3 The gateway routes IP addresses 199.203.73.64 to 199.203.73.80 to the internal interface (10.0.0.1).

## Gateway with Three Interfaces

## Hide Mode and Static Mode

Consider the following network and Address Translation configuration:

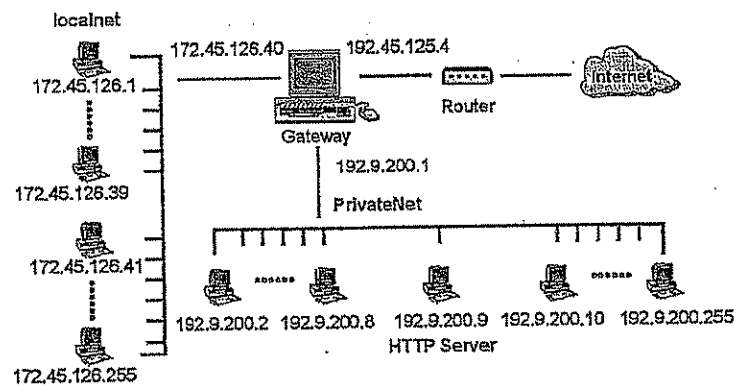


FIGURE 5-33 Gateway with Three Interfaces Example - Network

Suppose we wish to hide all the localnet and DMZ hosts behind the gateway, except for host 192.9.200.9 (HTTPServer), which will be providing public services and so must be accessible from the Internet.

Gateway with Three Interfaces

### Defining Address Translation

#### Hiding localnet

To hide localnet addresses, define Address Translation as follows for localnet:

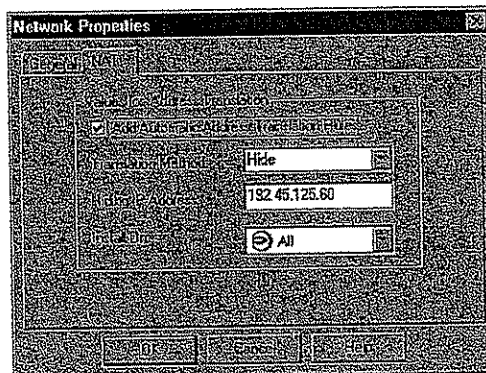


FIGURE 5-34 Hiding localnet

#### Hiding PrivateNet

To hide PrivateNet addresses, define Address Translation as follows for PrivateNet:

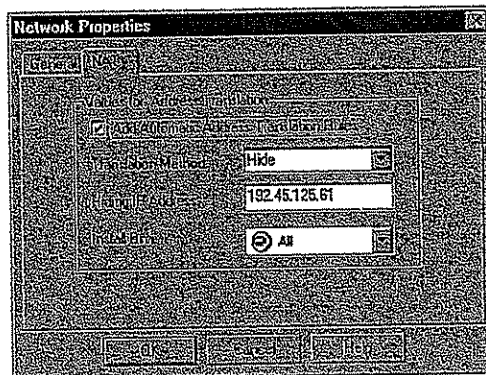


FIGURE 5-35 Hiding PrivateNet

## Address Translation Examples

## HTTPServer

To statically translate HTTPServer's address, define its Address Translation as follows:

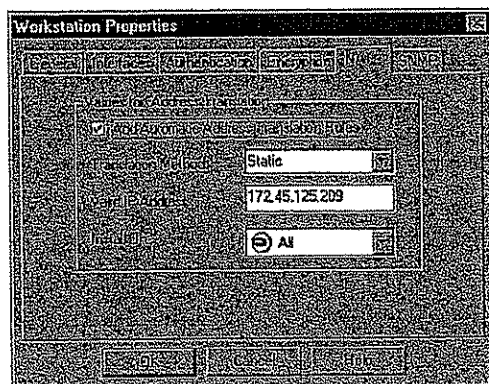


FIGURE 5-36 Translating HTTPServer

## Rules

The rules generated from these definitions is shown in FIGURE 5-37.

No.	Original Packet			Translated Packet			Install On
	Source	Destination	Service	Source	Destination	Service	
1	HTTPServer	Any	Any	HTTPServer (Valid Address)	Original	Original	All
2	Any	HTTPServer (Valid Address)	Any	Original	HTTPServer	Original	All
3	PrivateNet	PrivateNet	Any	Original	Original	Original	All
4	PrivateNet	Any	Any	PrivateNet (Hiding Address)	Original	Original	All
5	localnet	localnet	Any	Original	Original	Original	All
6	localnet	Any	Any	localnet (Hiding Address)	Original	Original	All

FIGURE 5-37 Automatically Generated Rules - Three Interfaces

Note that the Static Mode rules are positioned before the Hide Mode rules.

## Communications Between Hosts in Different Internal Networks

Address Translation works much like the Rule Base. The Address Translation rules are scanned sequentially, one after the other, until a match is found. The Address Translation indicated by the matching rule is performed, and then the packet is sent on its way.

## Gateway with Three Interfaces

Suppose host 172.45.126.47 (in localnet) tries to TELNET to host 172.45.125.209 (the valid address of HTTPServer (whose invalid address is 192.9.200.9) in PrivateNet. The first rule that matches is rule 2, so the destination address 172.45.125.209 is translated to 192.9.200.9, and the packet arrives at its destination. The packet's source address (172.45.126.47) remains untranslated, so the reply will be sent to 172.45.126.47 and arrive at its destination.

## Routing

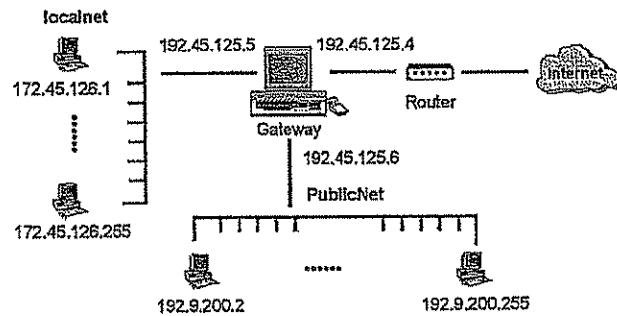
Assume that the Internet routes the IP addresses in the network 192.45.125.0 to the router.

Then you should ensure that:

- 1 The router routes the IP addresses in the network 192.45.125.0 to the gateway:
- 2 The gateway routes IP address 172.45.125.209 to the internal interface (192.9.200.1).

**Both Networks Statically Translated**

Consider the following network and Address Translation configuration:



**FIGURE 5-38** Three Interfaces - Both Networks Statically Translated



## Address Translation Examples

Suppose we wish to statically translate the addresses in both networks (localnet and PublicNet). The automatically generated Address Translation Rule Base is shown in FIGURE 5-39.

No.	Original Packet			Translated Packet			Install On
	Source	Destination	Service	Source	Destination	Service	
1	PublicNet	PublicNet	Any	Original	Original	Original	Any
2	PublicNet	Any	Any	PublicNet (Valid Addresses)	Original	Original	Any
3	Any	PublicNet (Valid Addresses)	Any	Original	PublicNet	Original	Any
4	localnet	localnet	Any	Original	Original	Original	Any
5	localnet	Any	Any	localnet (Valid Addresses)	Original	Original	Any
6	Any	localnet (Valid Addresses)	Any	Original	localnet	Original	Any

FIGURE 5-39 Rule Base - Both Networks Statically Translated

## Communications Between Hosts Behind the Same Gateway

Suppose a host in localnet tries to TELNET to a host in PublicNet, using the PublicNet host's valid IP address as the destination IP address. The first rule that applies is rule 3, so the destination address is translated and the packet is correctly routed to the destination. The reply packets are correctly routed as well, since the source IP address is not translated.


On the other hand, suppose a host in PublicNet tries to TELNET to a host in localnet, using the localnet host's valid IP address as the destination IP address. The first rule that matches is rule 2, so the source address is translated, but the destination address is not translated, so the packet will *not* arrive at its destination.



## Gateway with Three Interfaces

## Multiple Translation Rules

One solution is to add two rules before the automatically generated rules as follows:



No.	Original Packet			Translated Packet		
	Source	Destination	Service	Source	Destination	Service
1	PublicNetInvalid	localnetValid	Any	PublicNetValid	localnetInvalid	Original
2	localnetInvalid	PublicNetValid	Any	localnetValid	PublicNetInvalid	Original
3	PublicNet	PublicNet	Any	Original	Original	Original
4	PublicNet	Any	Any	PublicNet (Valid Address)	Original	Original
5	Any	PublicNet (Valid Address)	Any	Original	PublicNet	Original
6	localnet	localnet	Any	Original	Original	Original
7	localnet	Any	Any	localnet (Valid Address)	Original	Original
8	Any	localnet (Valid Address)	Any	Original	localnet	Original

FIGURE 5-40 Multiple Translation Rules Added to Automatically Generated Rules

Now, both source and destination IP addresses will be translated, so packets will be routed to their correct destinations.

## Simple Rules

Another solution is to add the same two rules, but to set **Source** under **Translated Packet** to **Original**. This solution will work because there is really no need to translate the source IP address when both networks are connected to the same gateway, which knows how to route to the internal invalid IP addresses of both networks.

## Communications Between Hosts Behind Different Gateways

Consider the case when the internal networks are connected to different gateways controlled from the same Management Station. In this case, both source and destination IP addresses must be translated, because each gateway knows how to route only to its own internal invalid IP addresses. Therefore, only the first of the above solutions (multiple translation rules) will work.

## Managing PIX Address Translation

PIX Address Translation can be manually configured through the FireWall-1 Address Translation Rule Base editor (Windows GUI). This method of configuration simplifies the management of PIX Address Translation.



**Note** – PIX does not support automatically generated Address Translation rules. Properties defined in the **NAT** tab of a network object are not applied. Address Translation rules installed on a PIX blackbox must be manually configured. See "Defining Address Translation Rules" on page 176 for more information.

## Managing PIX Address Translation

**Overview**

PIX performs address translation for the networks on its inside interface only. These networks must be specified as the "inside Addresses" in the Setup A tab of the Blackbox Properties window (Windows GUI). Addresses of hosts on the PIX outside interface are not translated.

PIX maps addresses of the inside hosts to a range of valid IP addresses, known as the PIX "Global Pool." PIX supports both the dynamic and static Address Translation modes, but manages these modes differently from FireWall-1.

**Dynamic**

In PIX dynamic Address Translation, a range of internal, or "inside" addresses is mapped to the Global Pool. Valid addresses are dynamically assigned to internal hosts per connection. Valid addresses are assigned according to availability and are returned to the global pool when a connection closes or times out.

For example, the 15 hosts of an internal network share a global pool of 10 valid addresses. If 10 hosts have connections open, then each of the remaining 5 hosts must wait until a connection times out in order to receive a valid address and open a connection.

For more information on PIX dynamic Address Translation and global pools, consult the Cisco PIX documentation.

**Static**

An invalid address from the inside private network is permanently mapped to a single valid address from the Global Pool. Static Address Translation is used for internal service hosts, such as an SMTP server. Static Mode ensures that a specific inside host can have unique, valid IP addresses.

## Using PIX in the Address Translation Rule Base

**Using PIX in the Address Translation Rule Base**

A subset of the FireWall-1 Address Translation Rule Base editor features are available for PIX. TABLE 5-13 compares the features supported by PIX and FireWall-1.

TABLE 5-13 Comparison of PIX and FireWall-1 in the Address Translation Rule Base

	PIX	FireWall-1
<b>Dynamic Address Translation (Hide Mode)</b>	A range of invalid addresses is dynamically mapped to a range of valid addresses (Global Pool).	Many invalid addresses are translated to a single valid address. The invalid addresses are "hidden" behind a single address. (see "Hide Mode" on page 159)
<b>Static Address Translation</b>	static source mode only	both static source and static destination mode
<b>compound conditions</b>	not available	available
<b>restrict rules to specific destination addresses</b>	not available	available
<b>multiple translation</b>	not available	available
<b>translate ports</b>	not available	available
<b>restrict rules to specific services</b>	not available Rules restricting connections to translated hosts are specified in the Security Policy Rule Base. See "PIX Address Translation Example" on page 202.	available

**Source**

Dynamic and static Address Translation is performed only for the objects listed under **Source** in both **Original Packet** and **Translated Packet**.

**Source** can consist of only one object. The types of objects allowed for **Source** under **Original Packet** depend on what is specified for **Source** under **Translated Packet**, as listed in TABLE 5-14.

TABLE 5-14 Original Packet - Source

	If Translated Packet - Source is ...		
	Original	Hide	Static
<b>Original Packet - Source can be ...</b>	Workstation or Address Range	Address Range	Workstation

## Managing PIX Address Translation

### Destination

The PIX blackbox does not allow you to specify rules to translate a packet's destination address in the Address Translation Rule Base. Connections from outside to inside hosts are enabled through the Security Policy Rule Base (see "PIX Address Translation Example" on page 202). When defining an Address Translation Rule Base, set **Destination** under **Original Packet** to **Any**. **Destination** under **Translated Packet** must be set to **Original**.

### Service

Rules which translate ports or restrict connections to specific services cannot be specified in the Address Translation Rule Base. Connections to inside hosts are restricted to specific services only through rules in the Security Policy Rule Base (see "PIX Address Translation Example" on page 202). When defining Address Translation rules, set **Service** under **Original Packet** to **Any**. **Service** under **Translated Packet** must be set to **Original**.

### Install On

Address Translation rules must be installed on the specific PIX blackbox that will enforce the rule. You must choose **Targets** from the **Install On** menu. The **Select Target** window (FIGURE 5-26 on page 187) is displayed, from which you can choose the PIX blackbox on which to install the Address Translation rule.

## PIX Address Translation Example

The following example describes how to define an Address Translation Rule Base for a single PIX blackbox with one network on the inside interface.

Consider the following configuration:

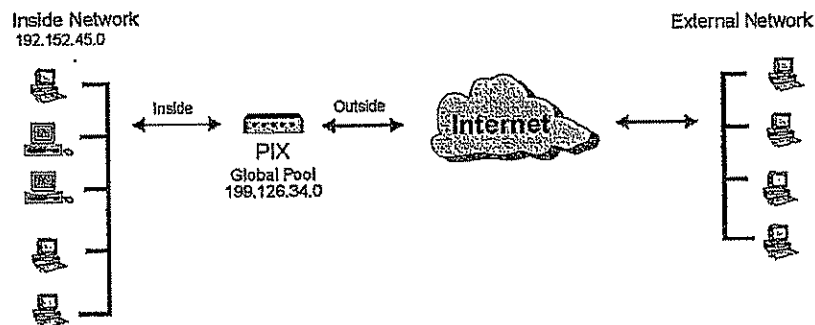


FIGURE 5-41 Example Configuration

To implement Address Translation for this configuration, you must first define two Address Range objects: one for the inside network and one for the PIX Global Range of addresses.

## PIX Address Translation Example

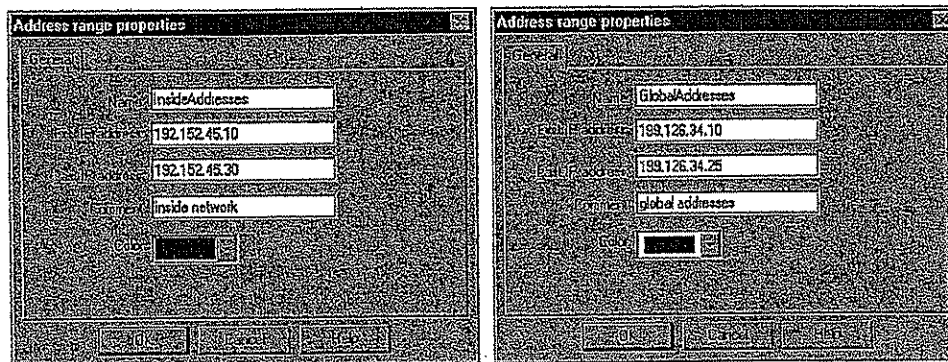


FIGURE 5-42 Address Range Properties — Inside Addresses and Global Addresses



**Note** – The Inside Network must already be specified as the PIX blackbox's **Inside Addresses** in the **Setup A** tab of the **Blackbox Properties** window (Windows GUI) or the **Blackbox Properties** window (OpenLook GUI).

Next, define a Hide Mode rule that dynamically maps the inside network (**Inside Addresses**) to the range of **GlobalAddresses**. This rule must be located first in the Address Translation Rule Base, before any other rules.

No.	Original Packet			Translated Packet			Install On
	Source	Destination	Service	Source	Destination	Service	
1							

FIGURE 5-43 Hide Mode rule

Note that in the Address Translation Rule Base, Hide Mode rules are used to dynamically map the inside network to the PIX Global Pool.

The first rule only enables inside hosts to initiate connections to external hosts. In order to allow connections from the outside to a specific inside host, you must statically assign a Global Address to that host. This assures that this host has a unique, valid address and can always be reached from the outside.



## Managing PIX Address Translation

To statically map a host, you must create two workstation objects: one specifying the host's internal address, and one with the host's Global Address (see FIGURE 5-44).

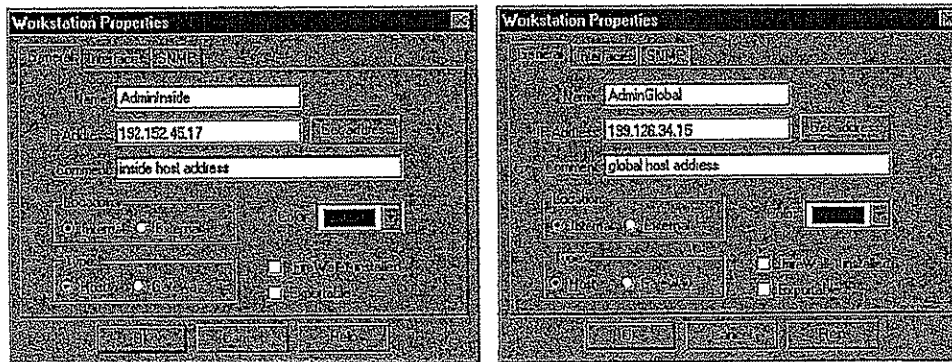


FIGURE 5-44 Workstation Properties — Inside Host and Corresponding Global Address

Next, define an Address Translation rule that statically translates packets from the inside host to its Global Address. The Address Translation rules below provide static Global Addresses for two hosts: **Admininside** and **InsideWeb**, a web server.

No	Original Packet			Translated Packet			Install On
	Source	Destination	Service	Source	Destination	Service	
1	Admininside	Any	Any	AdminGlobal	Any	Any	PIX
2	Admininside	Any	Any	AdminGlobal	Any	Any	PIX
3	InsideWeb	Any	Any	WebGlobal	Original	Original	PIX

FIGURE 5-45 Address Translation Rule Base with Static Address Translation rules



## Address Translation and Anti-Spoofing

You must then define rules in the Security Policy Rule Base that enable connections between the inside network and external hosts.

No.	Source	Destination	Service	Action	Track	Install On	Comment
1							
2							
3							
4	Any	ExtNet	Any	accept		FORT	

FIGURE 5-46 Security Policy Rule Base

- Rule 1 enables connections from hosts in an external network (Extnet) to any inside host with a Global address.
- Rule 2 enables Admininside to connect to any external host.
- Rule 3 enables any external host to access the web server.
- Rule 4 allows all hosts in the inside network to connect to a host on Extnet.

## Advanced Topics

### Address Translation and Anti-Spoofing

Anti-Spoofing examines the source IP address for incoming packets (entering a gateway), and the destination IP address for outgoing packets (leaving a gateway).

Anti-Spoofing is described in "Valid Addresses" on page 25 of *Managing FireWall-1 Using the Windows GUI* and in "Anti-Spoofing" on page 35 of *Managing FireWall-1 Using the OpenLook GUI*.

Address Translation takes place as follows:

- for a packet going from the client (the Initiator of the connection) to the server, just before the packet leaves the interface closest to the server
- for a packet going from the server to the client, just after the packet enters the interface closest to the server

### Automatically Generated Rules

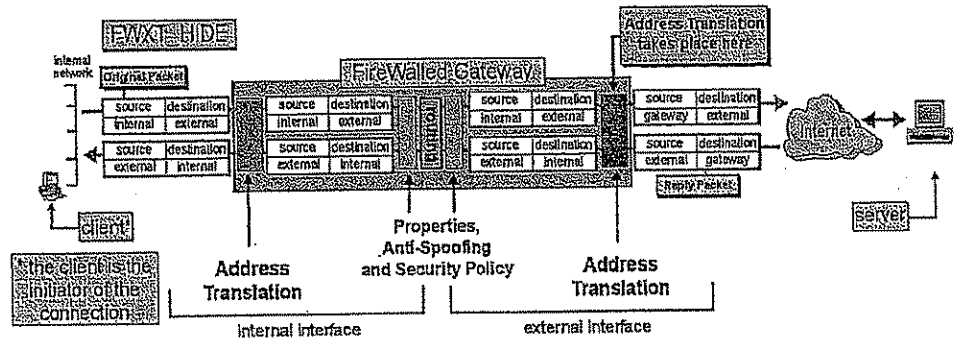
You do not have to do anything to ensure that anti-Spoofing is performed correctly for those objects for which you generate Address Translation rules automatically. There is one exception: for static destination mode translation, you must add the translated addresses to the internal interface's **Valid Addresses**. See "Static Destination Mode" on page 208 for more information about this case.

This remainder of this section describes anomalies which must be considered when you define Address Translation manually. The examples illustrate the interaction between Address Translation and Anti-Spoofing for each of the Address Translation modes.

## Advanced Topics

**Hide Mode**

FIGURE 5-47 shows a gateway performing both Address Translation (in Hide Mode) and Anti-Spoofing on a packet and its reply as they pass through the gateway.



**FIGURE 5-47** Address Translation and Anti-Spoofing (Hide Mode)

**Original Packet**

On the internal interface, Anti-Spoofing sees an incoming packet with an internal source IP address, which is normal.

On the external interface, Anti-Spoofing sees an outgoing packet with an external destination IP address, which is normal.

**Reply Packet**

On the external interface, Anti-Spoofing sees an incoming packet with an external source IP address, which is normal.

On the internal interface, Anti-Spoofing sees an outgoing packet with an internal destination IP address, which is normal.

**Conclusion**

In Hide Mode, there is no conflict between Address Translation and Anti-Spoofing.

## Address Translation and Anti-Spoofing

## Static Source Mode

FIGURE 5-48 shows a gateway performing both Address Translation (in Static Source Mode) and Anti-Spoofing on a packet and its reply as they pass through the gateway.

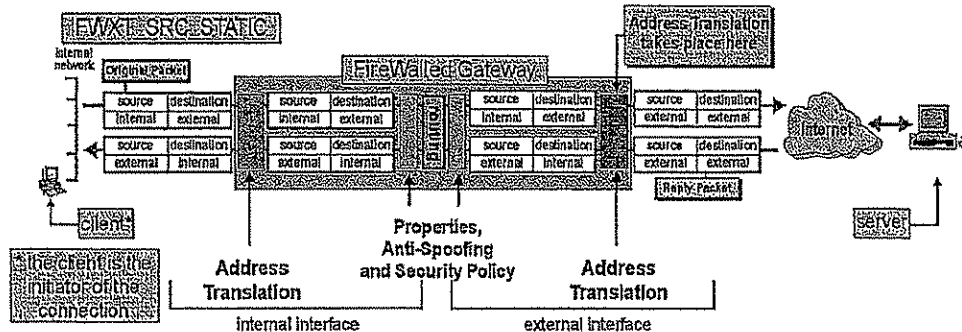


FIGURE 5-48 Address translation and Anti-Spoofing (Static Source Mode)

## Original Packet

On the internal interface, Anti-Spoofing sees an incoming packet with an internal source IP address, which is normal.

On the external interface, Anti-Spoofing sees an outgoing packet with an external destination IP address, which is normal.

## Reply Packet

On the external interface, Anti-Spoofing sees an incoming packet with an external source IP address, which is normal.

On the internal interface, Anti-Spoofing sees an outgoing packet with an internal destination IP address, which is normal.

## Conclusion

In Static Source Mode, there is no conflict between Address Translation and Anti-Spoofing.

## Advanced Topics

## Static Destination Mode

FIGURE 5-49 shows a gateway performing both Address Translation (in Static Destination Mode) and Anti-Spoofing on a packet and its reply as they pass through the gateway.

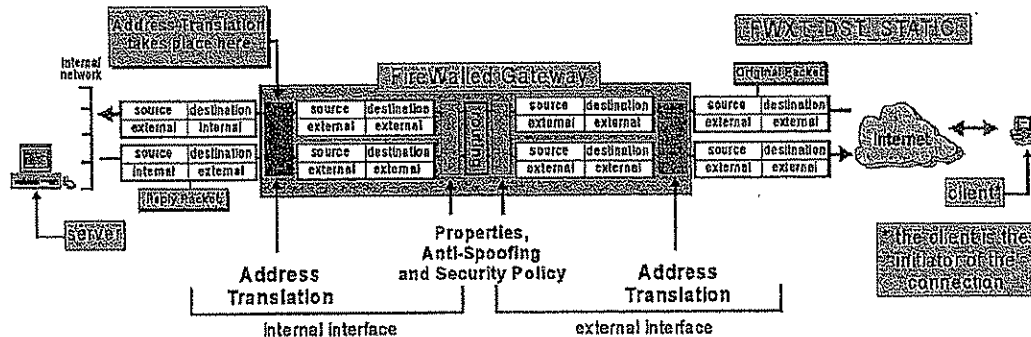


FIGURE 5-49 Address translation and Anti-Spoofing (Static Destination Mode)

## Original Packet

On the external interface, Anti-Spoofing sees an incoming packet with an external source IP address, which is normal.

On the internal interface, Anti-Spoofing sees an outgoing packet with an external destination IP address, which is *not* normal.

To correct the problem, add the translated (external) IP addresses to the **Valid Addresses** on the internal interface.

## Reply Packet

On the internal interface, Anti-Spoofing sees an incoming packet with an external source IP address, which is *not* normal.

To correct the problem, add the translated (external) IP addresses to the **Valid Addresses** on the internal interface.

On the external interface, Anti-Spoofing sees an outgoing packet with an external destination IP address, which is normal.

## Address Translation and Anti-Spoofing

## Example

Consider the following network and Address Translation configuration:

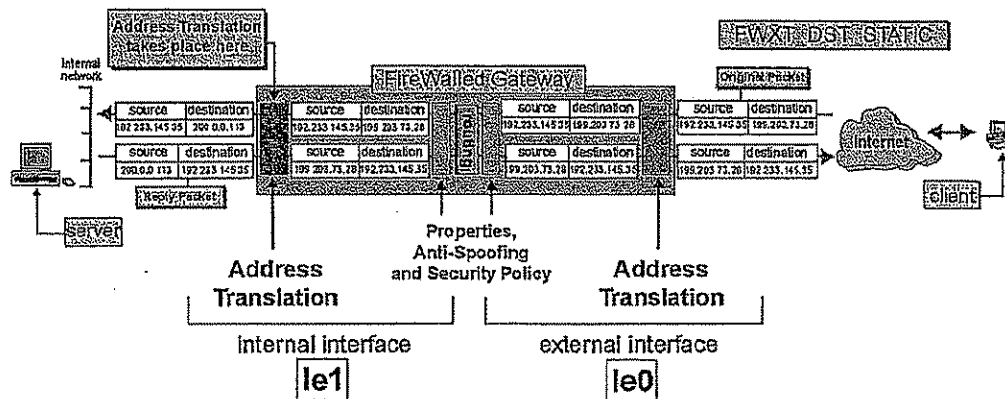


FIGURE 5-50 Address Translation and Anti-Spoofing (Example)

No.	From Original Address (Port)	To Original Address (Port)	Method	First Translated Address (Port)
0	199.203.73.15	199.203.73.115	FWXT_DST_STATIC	200.0.0.100

On the internal interface (le1), Anti-Spoofing sees outgoing packets with external destination IP addresses (199.203.73.15 – 199.203.73.115) and incoming packets with external source IP addresses (199.203.73.15 – 199.203.73.115). To prevent these packets from being identified as spoofed packets, you must add the translated addresses to the internal interface's **Valid Addresses**.

#### Defining Valid Addresses

- 1 Define a network object (for example, "localnet") for the invalid internal network (200.0.0.0).
- 2 Define a network object (for example, "xlnet") for the translated addresses (199.203.73.0).
- 3 Define a group (for example, "bothnets") which consists of localnet and xlnet.
- 4 For le1 (the internal interface), define the **Valid Addresses** as **bothnets**.
- 5 For le0 (the external interface), define the **Valid Addresses** as **Others**.

# **EXHIBIT 3**

## **PART 4**



## Frequently Asked Questions

## Rule Base



**Note** – This section describes anomalies which must be considered when you define Address Translation manually. If you generate Address Translation rules automatically, these considerations do not apply.

The Inspection Module sees the packet as the initiator of the connection sees it, and the Rule Base should be defined accordingly.

In the usual situation, this means that if the source (from the initiator's point of view) is an internal host and the destination an external one, then the source object in the rule should be the internal invalid address.

If, from the initiator's point of view, the source is an external host and the destination is an internal one, then the destination objects in the rule should be the external addresses of the FWXT\_DST\_STATIC translated hosts(s).

For example, consider the network configuration and Address Translation rules described in FIGURE 5-28 on page 191. A rule in the Rule Base that refers to incoming mail would specify the mail server (under **Destination**) as 199.203.73.3, because the initiator of the communication (the outside host) knows the mail server under that name (IP address).

On the other hand, a rule in the Rule Base that refers to outgoing mail would specify the mail server (under **Source**) as 10.0.0.2, because the initiator of the communication (the internal network) knows the mail server under that name (IP address).

## Frequently Asked Questions

Why do the translated addresses seem not to exist (I can't even ping them) even though the Address Translation configuration is correct?	page 210
Can I translate the gateway's internal address?	page 211
How can I use Encryption and Address Translation together on the same system?	page 213
What happens when an internal host with an invalid internal IP address tries to communicate with an external host that has the same IP address?	page 214
How can I overcome the limit on the number of lines in the file \$FWDIR/conf/xlate.conf?	page 215
How can I install different Address Translation configurations on different network objects controlled by the same Management Station?	page 216

Why do the translated addresses seem not to exist (I can't even ping them) even though the Address Translation configuration is correct?

You must modify the gateway's internal routing tables to enable this to happen.

Rule Base

Suppose the Address Translation is configured as follows:

No.	From Original Address (Port)	To Original Address (Port)	Method	First Translated Address (Port)
0	206.73.224.1	206.73.224.1	FWXT_SRC_STATIC	192.168.145.11
1	192.168.145.11	192.168.145.11	FWXT_DST_STATIC	206.73.224.1
2	206.73.224.85	206.73.224.85	FWXT_SRC_STATIC	192.168.145.12
3	192.168.145.12	192.168.145.12	FWXT_DST_STATIC	206.73.224.85

If you ping 192.168.145.11 (whether from outside your network or from inside it), then the gateway routes the ping request to its external interface and it is never received by 192.168.145.11. This is because the internal routing takes place before the Address Translation (see "Address Translation and Anti-Spoofing" on page 205).

In order to be able to ping 192.168.145.11 and 192.168.145.12, you must add static routes in the gateway which tell it to forward packets destined for 192.168.145.11 and 192.168.145.12 to the internal interface.

For additional information, see "Configuring Routing on the Gateway" on page 165.

Can I translate the gateway's internal address?



**Note** - This section describes anomalies which must be considered when you define Address Translation manually. If you generate Address Translation rules automatically, these considerations do not apply.

You should not translate the internal address (the address of the internal interface) of the translating gateway.

## Frequently Asked Questions

For example, consider the following network and Address Translation configuration:

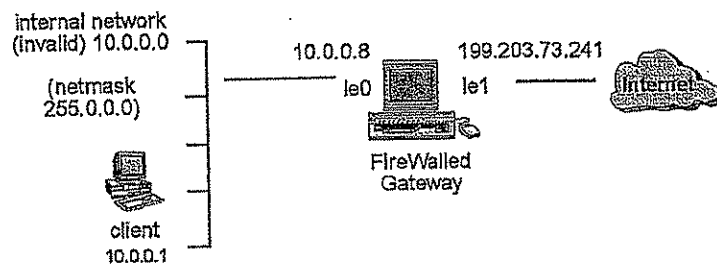


FIGURE 5-51 Hidden Internal Network

No.	From Original Address (Port)	To Original Address (Port)	Method	First Translated Address (Port)
0	10.0.0.1	10.255.255.255	FWXT_HIDE	199.203.73.200

This example shows a simple translation scheme that hides the entire internal network, whose addresses are invalid, behind a valid address. The problem with this configuration is that the FireWalled gateway's internal address (10.0.0.8) is also translated to the gateway's external address, since 10.0.0.8 is in the range 10.0.0.0 - 10.255.255.255. An attempt to communicate from the gateway to an internal machine will not succeed.

For example, if you TELNET from the gateway to 10.0.0.1, the gateway's internal address (10.0.0.8) will be translated to 199.203.73.200. The reply packet will not reach its destination, because 10.0.0.1 will not be able to route the reply to 199.203.73.200.

To solve this problem, use the following address translation scheme, which translates all the addresses except the gateway's address:

No.	From Original Address (Port)	To Original Address (Port)	Method	First Translated Address (Port)
0	10.0.0.1	10.0.0.7	FWXT_HIDE	199.203.73.200
1	10.0.0.9	10.255.255.255	FWXT_HIDE	199.203.73.200

## Rule Base

How can I use Encryption and Address Translation together on the same system?



**Note** – You do not have to do anything to ensure that Encryption is performed correctly for those objects for which you generate Address Translation rules automatically. This section describes anomalies which must be considered when you define Address Translation manually.

For example, suppose you want to encrypt between Network-A and Network-B, where Network-A uses invalid addresses translated as follows:

No.	From Original Address (Port)	To Original Address (Port)	Method	First Translated Address (Port)
0	10.1.1.2	10.1.1.2	FWXT_SRC_STATIC	192.91.18.2
1	192.91.18.2	192.91.18.2	FWXT_DST_STATIC	10.1.1.2
2	10.1.1.3	10.1.1.255	FWXT_HIDE	192.91.18.3

Network-B uses the valid addresses of network 195.8.5.0.

FireWall-A (Network-A's FireWall) should specify as its Encryption Domain both the invalid addresses (10.1.1.x) and the valid addresses (192.91.18.x).

FireWall-B (Network-B's FireWall) knows FireWall-A only by its valid address.

## Encryption Rules

On FireWall-A, two Encryption rules are needed:

Source	Destination	Services	Action	Track	Install On
10.1.1.0	195.8.5.0	Any	Encrypt	Short Log	Gateways
195.8.5.0	192.91.18.0	Any	Encrypt	Short Log	Gateways

As with all Address Translation, the Inspection Module see the packets as the originator of the connection sees it, so the first rule applies to outgoing connections and the second rule applies to incoming connections.

Two Encryption rules are needed on FireWall-B as well:

Source	Destination	Services	Action	Track	Install On
192.91.18.0	195.8.5.0	Any	Encrypt	Short Log	Gateways
195.8.5.0	192.91.18.0	Any	Encrypt	Short Log	Gateways

## Frequently Asked Questions

Here too the first rule applies to outgoing connections and the second rule applies to incoming connections, but the same addresses are used in both rules, since FireWall-B doesn't know about Network-A's invalid addresses.

The sequence of actions between Network-A and Network-B is as follows (for a connection from Network-A to Network-B):

- 1 The packet is encrypted by FireWall-A.
- 2 The packet's source IP address is translated by FireWall-A.
- 3 The packet is decrypted by FireWall-B.
- 4 The return packet is encrypted by FireWall-B.
- 5 The return packet's destination IP address is translated by FireWall-A.
- 6 The return packet is decrypted by FireWall-A.

What happens when an internal host with an invalid internal IP address tries to communicate with an external host that has the same IP address?

In this case, the internal network does not conform to the IANA recommendations (see "Frequently Asked Questions" on page 210) but instead uses IP addresses that "belong" to another network.

Consider what happens when the internal host 129.1.1.1 in FIGURE 5-52 tries to talk to the external host 129.1.1.1.

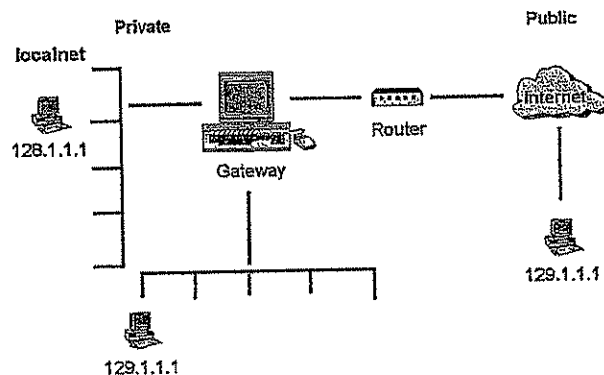


FIGURE 5-52 Invalid IP Addresses

The outbound packet will remain in the host, since it looks like this:

Source IP Address	Destination IP address
129.1.1.1	129.1.1.1

## Rule Base

The host will route the packet right back to its itself, and the packet will never reach the gateway.

If the internal host 128.1.1.1 tries to talk to the external host 129.1.1.1, the gateway will route the communication to the internal host 129.1.1.1 (connected to the gateway through another interface) rather than to the external host 129.1.1.1.

Using FWXT\_HIDE to hide the invalid IP addresses behind the gateway's valid address will not help, because with FWXT\_HIDE the Address Translation takes place on the gateway's external interface. The packet will not get that far because it will have been routed to the other internal interface (see "Address Translation and Anti-Spoofing" on page 205).

How can I overcome the limit on the number of lines in the file  
\$FWDIR/conf/xlate.conf?



**Note** - This section describes anomalies which must be considered when you define Address Translation manually. If you generate Address Translation rules automatically, these considerations do not apply.

There is no limit to the number of lines in \$FWDIR/conf/xlate.conf, but the fwxcnf utility does not handle files with more than 98 lines.

\$FWDIR/conf/xlate.conf is an ASCII file that can be manually edited, using any ASCII editor.

You can use fwxcnf to configure the first 98 entries and then manually edit \$FWDIR/conf/xlate.conf to add additional entries. Edit only the following table:

```
fwx_translation={
    ...
};
```

Here is an example of an fwx\_translation table:

```
fwx_translation={
    <0, 10.0.0.1, 10.255.255.250,FWXT_HIDE, 198.161.99.3, 0>,
    <1, 11.1.1.3, 11.1.1.3,FWXT_SRC_STATIC, 198.161.99.4, 0>,
    <2, 198.161.99.4,198.161.99.4,FWXT_DST_STATIC,11.1.1.3,0>,
};
```



## Frequently Asked Questions

The fields in the `fwx_translation` table have the following meanings:

TABLE 5-15 `fwx_translation` table - meaning of fields

Field No.	Meaning
1	entry id (a sequence number starting at 0)
2	start of the address range
3	end of the address range
4	method
5	translated address
6	always 0, not used

Except for the first and last fields, the fields correspond to the fields in the input to `fwx1.conf`.

How can I install different Address Translation configurations on different network objects controlled by the same Management Station?

If you are using the Windows GUI, then you can do this by specifying different network objects in the **Install On** field in the network object's NAT tab, or in the **Install On** field of a manual Address Translation rule (see "Install On" on page 186).

Otherwise, you must manually edit `$FWDIR/conf/xlate.conf`. An automatically generated `$FWDIR/conf/xlate.conf` file has only one translation table, as follows:

```
fwx_translation = {
  <0, 172.1.0.2, 172.1.0.2, FWXT_HIDE, 192.168.207.5, 0>,
};
```

You must create a separate translation table for each gateway. For example:

```
fwx_translation_tinker = {
  <0, 172.1.0.2, 172.1.0.2, FWXT_HIDE, 192.168.207.5, 0>;
fwx_translation_evers = {
  <0, 10.2.0.2, 10.2.0.2, FWXT_HIDE, 192.168.210.130, 0>;
fwx_translation_chance = {
  <0, 10.1.0.2, 10.1.0.2, FWXT_HIDE, 192.168.217.2, 0>;
```

## Rule Base

Next, you must associate each table with the gateway on which it is to be installed. For example (<> means eitherbound):

```
<> all@tinker
  set srl5 fw_x_translation_tinker;
<> all@evers
  set srl5 fw_x_translation_evers;
<> all@chance
  set srl5 fw_x_translation_chance;
```

Here is an example of a complete \$FWDIR/conf/xlate.conf file:

```
#define FWXT_HIDE 0x1
#define FWXT_SRC_STATIC 0x2
#define FWXT_DST_STATIC 0x202
#define FWXT_DPORT_STATIC 0x302

#define FWXLATE_ACTIVE 1
fw_x_translation_tinker={
  <0, 172.1.0.2, 172.1.0.2, FWXT_HIDE, 192.168.207.5, 0>,
};

fw_x_translation_evers={
  <0, 10.2.0.2, 10.2.0.2, FWXT_HIDE, 192.168.210.130, 0>
};

fw_x_translation_chance={
  <0, 10.1.0.2, 10.1.0.2, FWXT_HIDE, 192.168.217.2, 0>,
};
#define FWXT_ON_ALL_HOSTS
FWXT_ON_ALL_HOSTS
#define FWXT_ON_ALL_IFS
FWXT_ON_ALL_IFS
<> all@tinker
  set srl5 fw_x_translation_tinker;
<> all@evers
  set srl5 fw_x_translation_evers;
<> all@chance
  set srl5 fw_x_translation_chance;
```

## Frequently Asked Questions

**CHAPTER 6**

# Routers and Embedded Systems

---

**In This Chapter**

<i>Overview</i>	<i>page 219</i>
<i>Routers and Blackboxes</i>	<i>page 220</i>
<i>Embedded Systems</i>	<i>page 221</i>

**Overview**

A FireWall-1 enforcement point is a machine or device that enforces at least some part of the Security Policy. An enforcement point can be a workstation, router, switch or any machine that can be managed by a Management Module by installing a Security Policy or Access List.

FireWall-1 includes the following types of enforcement points:

- Routers and Blackboxes
- Embedded systems

## Overview

**Routers and Blackboxes**

Routers include hardware and software packet filters. A blackbox is a hardware routing device which provides additional security features, such as Network Address Translation and Authentication. The Management Module generates Access Lists from the Security Policy and downloads them to selected routers and blackboxes.

TABLE 6-1 summarizes the FireWall-1 features supported by managed routers and blackboxes.

**TABLE 6-1** Routers and Blackboxes - supported FireWall-1 features

Platform and Version	Accept/Reject Rules	Anti-Spoofing	Properties	Logs and Alerts <sup>4</sup>	Implicit Last "Reject All" Rule	FTP Data Connections <sup>5</sup>
Bay Networks Router	Y	Y	Y	Y	Y	
3Com Router	Y	Y	Y	Y	Y	Y
Cisco Router 9	Y	N	Y	Y	Y	
Cisco Router 10.x and higher <sup>1</sup>	Y	Y	Y	Y	Y	
Cisco PIX Blackbox	Y	N	N	Y	Y	
Microsoft Steelhead <sup>6</sup>	Y <sup>2</sup>	N	Y <sup>3</sup>	N	Y <sup>3</sup>	N

1. In the FireWall-1 GUI, you can configure Cisco Version 11 routers as Version 10, but this is optional.

2. Action is defined per Policy. You cannot have Accept and Reject rules in the same Policy.

3. Relevant only for a Policy with Accept rules.

4. This is done using the router's syslog service.

5. This column indicates whether an FTP rule apply to the data connection as well as to the control connection. If the FTP rule does not apply, some other mechanism must be found for allowing the data connection (perhaps by opening all the high ports).

6. Microsoft Steelhead is supported by the Windows GUI only.

A Bay Networks router can function in either of two modes: as a packet filter (in which case FireWall-1 installs Access Lists on the router), or as an embedded system, (in which case FireWall-1 installs a Security Policy on the router). For more information, see TABLE 6-2 on page 222.

Embedded Systems

## Embedded Systems

Embedded systems include machines or hardware devices on which a FireWall Module or an Inspection Module is installed. Inspection Code is generated from the Security Policy and downloaded to targeted devices. Embedded systems implement different FireWall-1 features, depending on whether a FireWall Module or an Inspection Module is installed.

FIGURE 6-1 depicts the relationship between FireWall Module and Inspection Module features.

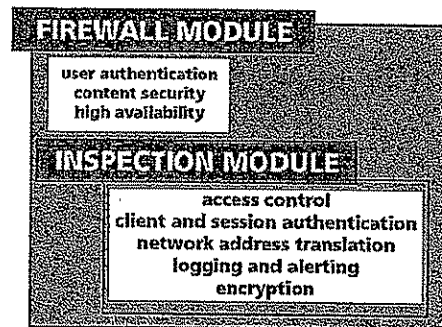


FIGURE 6-1 FireWall and Inspection Modules

The FireWall Module includes the Inspection Module, the FireWall-1 Security Servers (which implement Content Security and User Authentication), and the FireWall Synchronization feature. The Inspection Module implements the Security Policy, logs events, and communicates with the Management Module using the daemons.



## Overview

TABLE 6-2 summarizes the FireWall-1 features supported by embedded systems.

**TABLE 6-2** Embedded Systems - supported FireWall-1 feature

Platform and Version	Inspection Module (I)/ FireWall Module (F)	Anti-Spoofing	Logs and Alerts	Session and Client Authentication	Network Address Translation (NAT)	Encryption	Accounting	Content Security	Time Objects
Bay Networks 11.02	I	Y <sup>1</sup>	Y	N	N	N	N	N	N
Bay Networks 12.00	I	Y <sup>1</sup>	Y	N	N	N	N	N	N
Xylan Switch	I	Y	Y	N	N	N	N	N	N
TimeStep PERMIT/Gate	I	Y	Y	Y	Y	N <sup>4</sup>	N	N	N
Nokia IP Routing (Ipsilon)	F	Y	Y	Y	Y	Y <sup>2</sup>	Y	Y <sup>3</sup>	Y

1. Interface names on Bay routers are incorrectly retrieved by Get, and must be modified manually. This will be corrected for the next Bay version (12.10)

2. Does not support SKIP

3. Content Security includes the following FireWall-1 features:

- Resources (FTP, URI, SMTP)
- User Authentication
- CVP and UPF Server Objects

4. TimeStep encryption features are available on PERMIT/Gate versions 2515 and 4515

The following is true for all embedded systems, regardless of the settings in **Control Properties (Properties Setup)** window.

- **Apply Gateway Rules to Interface Direction** is always **Eitherbound**
- **FASTPATH** is always enabled

---

**CHAPTER 7**

---

# Management Server

---

## In This Chapter

<i>FireWall-1 Client/Server Structure</i>	<i>page 223</i>
<i>Client/Server Interaction</i>	<i>page 224</i>
<i>Access Control</i>	<i>page 225</i>

## FireWall-1 Client/Server Structure

### FireWall-1 Modules

FireWall-1 is comprised of two primary modules:

#### Management Module

The Management Module includes the Graphical User Interface (GUI) and the Management Server.

The GUI is the front end to the Management Module, which manages the FireWall-1 database: the Rule Base, network objects, services, users etc.

#### FireWall Module

The FireWall Module includes the Inspection Module and FireWall-1 daemons.

The FireWall Module implements the security policy, logs events, and communicates with the Management Module using the daemons.

## Client/Server Interaction

## Client/Server

The two components of the Management Module (the GUI and the Management Server) can be installed on the same machine or on two different machines. When they are installed on two different machines, FireWall-1 implements the Client/Server model, in which a GUI Client running on a Windows or X/Motif workstation controls a Management Server running on a Windows or Unix workstation.

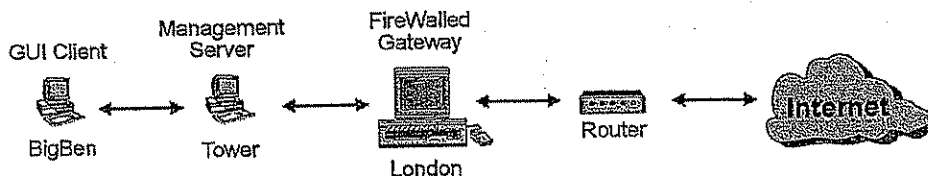


FIGURE 7-1 FireWall-1 Client-Server configuration

In the configuration depicted in FIGURE 7-1, the functionality of the Management Module is divided between two workstations (Tower and BigBen). The Management Server, including the FireWall-1 database is on Tower, the server. The GUI is on BigBen.

The user, working on BigBen, maintains the FireWall-1 Security Policy and database, which reside on Tower. The FireWall Module is installed on London, the FireWalled gateway, which enforces the Security Policy and protects the network.

The Management Server is *fwm* (see "fwm" on page 279), which is also used for adding, updating and removing administrators. *fwm* must be running on the Management Server computer if you wish to use the GUI client on one of the client machines.

## Client/Server Interaction

A GUI Client can manage the Server (that is, run the GUI Client to communicate with a Management Server) only if both the administrator running the GUI Client and the machine on which the GUI Client is running have been authorized to access the Management Server.

In practice, this means that the following conditions must both be met:

- 1 The machine on which the Client is running is listed in the `$FWDIR/conf/gui-clients` file.

If your Management Server is running under Windows NT, you can add or delete GUI Clients using the FireWall-1 Configuration application. See Chapter 2, "Installing FireWall-1," of *Getting Started with FireWall-1* for information about the FireWall-1 Configuration application.

## Concurrent Sessions

If your Management Server is running under Unix, then you can add or delete GUI Clients by using any text editor to modify `$FWDIR/conf/gui-clients` directly. The file consists of IP addresses or resolvable names, one per line. Alternatively, you can use the `fwconfig` script.

- 2 The administrator (user) running the GUI has been defined to the Management Server.

If your Management Server is running under Windows NT, you can add or delete administrators using the FireWall-1 Configuration application. See Chapter 2, "Installing FireWall-1," of *Getting Started with FireWall-1* for information about the FireWall-1 Configuration application.

If your Management Server is running under Unix, then you can add or delete administrators using the `-a` and `-r` options of the `fwm` program. See "fwm" on page 279 for information about the `fwm` program. Alternatively, you can use the `fwconfig` script.

## Access Control

Administrators are assigned access privilege levels, as listed in TABLE 7-1, beginning with the least-privileged level. Each privilege level has the privileges of all the lower privilege levels.

TABLE 7-1 Privilege Levels

	Access Privilege Level	Privileges
1	Monitor Only	access only the Log Viewer and System Status
2	Read Only	read-only access to the Security Policy Editor
3	User Edit	can modify user data
4	Read/Write	full read-write access

Whenever an administrator logs in, all his or her actions are recorded on the Management Server in a file called `$FWDIR/fwui.log`.

## Changing Privileges

You can change an administrator's privileges by using the `-a` option of the `fwm` program. See "fwm" on page 279 for information about the `fwm` program.

If your Management Server is running under Windows NT, you can modify an administrator's privileges by using the FireWall-1 Configuration application. See Chapter 2, "Installing FireWall-1" of *Getting Started with FireWall-1* for information about the FireWall-1 Configuration application.

## Concurrent Sessions

In order to prevent more than one administrator from modifying a Security Policy at the same time, FireWall-1 implements a locking mechanism.

## Access Control

Any number of administrators can view a Security Policy at the same time, but only one of them can have write permission at any given moment. Upon opening a Security Policy, an administrator is granted write permission only if both of the following conditions are true:

- the administrator has been assigned a Read/Write or User Edit privileges (see "Access Control" on page 225)
- no other administrator currently has write permission for the Security Policy at this time

For example, suppose Bob and Alice are both administrators. Bob has Read/Write privileges and Alice has User Edit privileges. Suppose no one has the Security Policy Editor open. If Alice opens the Security Policy Editor, she will be granted User Edit permission. If Bob opens the same Security Policy before Alice closes it on her workstation, then Bob will not be granted Read/Write permission. Instead, he will be asked whether he wishes to quit or to open the Security Policy with Read Only permission.

## Read Only Sessions

An administrator with Read/Write or User Edit privileges can open a Read Only session by checking the **Read Only** checkbox in the **FireWall-1 Security Policy Login** window (FIGURE 7-2).

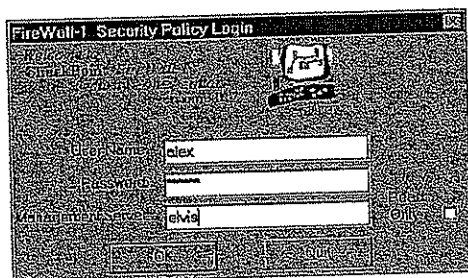


FIGURE 7-2 Login window

During the Read Only session, another administrator with Read/Write privileges can log in and be granted write permission.

## Locking

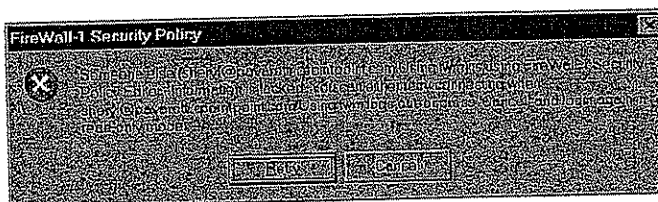
For configurations where the OpenLook GUI (fwui) is used, FireWall-1 provides a locking mechanism to avoid concurrency problems.

When fwui starts, it creates a file named `manage.lock` in the directory `$FWDIR/log`. When fwui terminates, it deletes the file.

If a `manage.lock` file already exists when fwui starts, then either another user is currently updating the Security Policy, or a previous instance of fwui (or fwm) terminated abnormally and failed to delete the `manage.lock` file.

## Locking

In this event, fwui displays an error message (giving the name of the process that created `manage.lock`), as in FIGURE 7-3.



**FIGURE 7-3** Security Policy locked message

Before you proceed, you must determine whether another user is currently using either the OpenLook or the Windows GUI to modify the Security Policy. You should do this in consultation with your system administrator, because the other user (if there is one) may be working at another location.

If someone else is currently modifying the Security Policy, then wait until that user is finished before resuming your own work. Otherwise, take one of the following actions:

- Remove the lock (that is, delete the `manage.lock` file).
- Terminate the other process (if it is still running).

In any case, it is best to consult your system administrator before proceeding.



**Note** – You may also wish to consider changing your management procedures to preclude the possibility of two people being able to modify your organization's Security Policy without coordinating their activities.



Access Control

228 FireWall-1 Architecture and Administration • September 1998

CHAPTER **8**

# Active Network Management

## In This Chapter

<i>FireWall Synchronization</i>	<i>page 229</i>
<i>Load Balancing</i>	<i>page 234</i>
<i>Connection Accounting</i>	<i>page 240</i>
<i>Active Connections</i>	<i>page 240</i>

## FireWall Synchronization

FireWall-1 provides Stateful Inspection even for stateless protocols such as UDP and RPC. To do this, the Firewall Module creates a virtual state for such connections, and updates this state according to the data transferred. In addition, FireWall-1 maintains state information for Address Translation and Encryption.

Different FireWall modules running on different machines can share this information and can mutually update each other with the different states of the connections.

FireWall Synchronization provides two benefits:

### **1** High Availability

When one of the FireWalled gateways stops functioning and another one takes its place, the second FireWalled gateway has the updated state of the first FireWalled gateway's connections, so the connections can be maintained.

## FireWall Synchronization

## 2 Different Routes for Connections

The IP protocol supports a network configuration in which packets sent from host A to host B may be routed through gateway C, while all packets sent from host B to host A may be routed through gateway D.



**Note** – FireWall-1 provides the mechanism for synchronizing the states of the FireWall Modules, but does not provide the mechanism for detecting failures and changing routing, etc..

## Implementation

The file `$FWDIR/conf/sync.conf` lists the other FireWall Modules (in the form of IP addresses or resolvable names) to which this FireWall Module sends its state information.

A control path must be established between all the FireWall Modules (using the `fw putkey` command), if one does not already exist.

When one FireWall Module goes down, the other FireWall Modules take over after the routing is re-configured.

## Example

FIGURE 8-1 shows a configuration in which two FireWalls (London and Paris) protect a network.

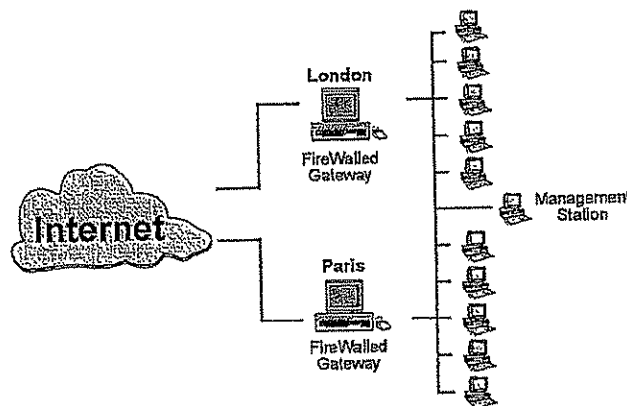


FIGURE 8-1 Two FireWalls in Synchronized Configuration

Example

## ▼ To configure London and Paris as synchronized FireWalls

On London

- 1 Create a file `$FWDIR/conf/sync.conf` containing one line:

```
Paris
```

- 2 Stop FireWall-1 by typing `fwstop`.
- 3 Establish a control path from London to Paris using the `fw putkey` command.  
You must do this only if there is not already a control path between London and Paris.  
For information on how to use the `fw putkey` command, see "fw putkey" on page 261.
- 4 Start FireWall-1 by typing `fwstart`.

On Paris

- 1 Create a file `$FWDIR/conf/sync.conf` containing one line:

```
London
```

- 2 Stop FireWall-1 by typing `fwstop`.
- 3 Establish a control path from Paris to London using the `fw putkey` command.  
You must do this only if there is not already a control path between London and Paris, as follows:  
On London, type:

```
fw putkey Paris <the authentication password (key)>
```

On Paris, type:

```
fw putkey London <the authentication password (key)>
```

- For information on how to use the `fw putkey` command, see "fw putkey" on page 261. For a detailed example of establishing control paths between computers, see "Synchronizing Authentication Passwords" on page 351.
- 4 Start FireWall-1 by typing `fwstart`.

## FireWall Synchronization

London and Paris will now begin to exchange the necessary state information to enable each of them to take the other's place if one of them goes down.

On the Management Station

Since the Management Station is not a FireWall, you do not have to do anything on the Management Station. Specifically, do not create a `$FWDIR/conf/sync.conf` file.

## Timing Issues

Synchronized FireWall Modules update each other with their state information approximately every 100 milliseconds.

The time on the synchronized Firewalls must be within seconds of each other. You should install some software that keeps the time synchronized between the two machines. Under Solaris2, you can use `xntpd`.

If one of the FireWall Modules goes down, the other FireWall Module may be unaware of connections initiated by the first FireWall Module in the 50 milliseconds before it went down. These connections will probably be lost.

If the FireWall Synchronization feature is being used to implement different routes in and out of a network (see "Different Routes for Connections" on page 230), then the following situation may arise (refer to FIGURE 8-1 on page 230):

One of the local network's computers initiates a connection to the Internet through London. The reply comes back through Paris. If the reply had come through London, it would have been allowed because the connection is in London's connection table. However, if the reply arrives before London and Paris synchronize their state information, then Paris will be unaware of connection, and will not allow the reply to pass.

The solution to this problem is for the Rule Base to drop these packets instead of rejecting them. When a TCP packet is dropped, no reset is sent to the packet's sender, so the sender will simply resend the packet after a delay. During this delay, London and Paris will have synchronized their states, so the packet will be allowed to pass on the second try.

These packets will be logged if the **Log Established TCP Packets** property is checked.

This solution is effective only for TCP.

## Restrictions

The following restrictions apply to synchronizing FireWall Modules:

### General

- 1 Only FireWall Modules running on the same platform can be synchronized.

For example, it is not possible to synchronize a Windows NT FireWall Module with a Solaris2 FireWall Module.

## Restrictions

- 2 The FireWall Modules must be the same software version.

For example, it is not possible to synchronize a Version 3.0 FireWall Module with a Version 4.0 FireWall Module.

- 3 The FireWall Modules must have the same Security Policy installed.

For example, suppose one FireWall Module accepts FTP and the other rejects FTP. If an FTP connection is opened through the first FireWall Module, the reply packets returning through the second FireWall Module will be accepted because the FTP connection is in the connections table. This behavior is inconsistent with the Security Policy on the second FireWall.

**Encryption**

- 4 Encrypted connections between two synchronized FireWall Modules do not function properly.
- 5 The SKIP key management protocol cannot be used on a synchronized FireWalled gateway.

**Address Translation**

- 6 If you are performing Network Address Translation with synchronized Firewalls, you must think very carefully about the routing. If the routing through the Firewalls is asymmetric (that is, if packets go out through one Firewall and replies return through the other), then you must make sure that routers on either side of the Firewall take into account the statically translated addresses.

Similarly, with the hidden IP addresses, you must think about which Firewall should be answering the ARP requests for those IP addresses.

**Authentication**

- 7 An authenticated connection through a FireWall Module will be lost if the FireWall Module goes down. Other synchronized FireWall Modules will be unable to resume the connection.
- 8 Authenticated connections will not work in the case where the synchronized feature is being used to implement different routes in and out of a network (see "Different Routes for Connections" on page 230).

The reason for these restrictions is that FireWall-1 authentication is implemented by Security Servers, which are processes, and thus cannot be synchronized on different machines in the way that data can be synchronized.

**Resources**

The state of connections using resources is maintained in a Security Server, so these connections cannot be synchronized for the same reason that authenticated connections cannot be synchronized.



## Load Balancing

### Accounting

- 9 If two FireWalls act as backups for each other, then accounting data cannot be accurately maintained by both FireWalls.

### SecuRemote

- 10 SecuRemote connections cannot be synchronized.

### Troubleshooting

Snoop ports 256 to see the communication activity between the two FireWalls. If the machines are synchronizing properly you will see:

- A message about them being connected on fwstart.
- An exchange of information every 50 milliseconds.

If you disconnect one FireWall from the network, the other FireWall should notice this.

## Load Balancing

### The Need for Load Balancing

The FireWall-1 Load Balancing feature enables several servers providing the same service to share the load among themselves.

Consider the configuration depicted in FIGURE 8-2 on page 235. All the HTTP servers can provide the HTTP client with the same services. Note that not all of the HTTP servers are behind the FireWalled gateway. In the same way, all the FTP servers can provide the FTP client with the same services.

## How Load Balancing Works

The system administrator wishes to ensure that the service load is balanced among the servers. The client will be unaware of the different servers. From the client's point of view, there is only one HTTP server and only one FTP server. When the service request reaches the gateway, FireWall-1 determines which of the servers will fulfill the request, based on the load balancing algorithm specified by the system administrator.

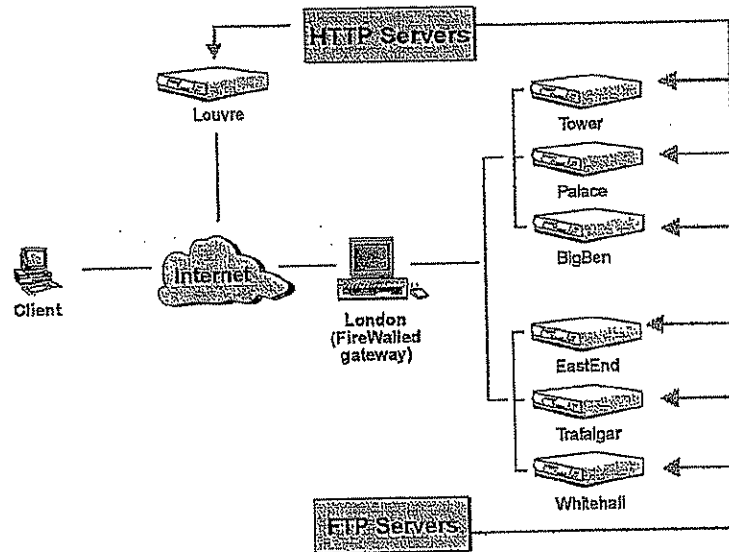


FIGURE 8-2 Load Balancing among several servers

**Note** – The IP address returned by the DNS should be the IP address of the Logical Server, to allow the FireWall to perform the load balancing between the physical servers.

## How Load Balancing Works

### HTTP

When HTTP is chosen under **Servers Type** in the **Logical Server Properties** window, Load Balancing is performed as follows:

- 1 FireWall-1 detects a service request for a Logical Server (see “Logical Servers” on page 237).

For example, the client starts an HTTP session on the Logical Server **HTTP\_servers** (whose **Server** is defined as **HTTP\_Group**, consisting of the servers **Tower**, **Palace** and **BigBen**, as shown in FIGURE 8-2 on page 235).

- 2 FireWall-1 determines that the session is to be redirected to a particular server.

## Load Balancing

For example, FireWall-1 determines, on the basis of the load balancing algorithm defined for the Logical Server **HTTP\_Servers**, that BigBen will be the server for this session.

- 3 FireWall-1 redirects the connection to the Load Balancing daemon (**lhttpd**).  
This is done using the translate port feature of the Address Translation mechanism.
- 4 FireWall-1 notifies the client that the URL is being redirected to the chosen server.  
This is done using the URL Redirection feature of HTTP to redirect the client to a specific IP address rather than the IP address of the Logical Server.
- 5 The rest of the session is conducted between the client and the chosen server, without the intervention of FireWall-1.

When **Other** is chosen under **Servers Type** in the **Logical Server Properties** window, Load Balancing for HTTP is performed using the Address Translation mechanism (as described in "Non-HTTP" on page 236). Each HTTP connection is then handled separately, and connections may be redirected to different servers. This may cause problems in some cases, for example, in an application where a user fills in a number of HTTP forms and a single server is expected to process all the data.

## Non-HTTP

- 1 FireWall-1 detects a service request for a Logical Server (see "Logical Servers" on page 237).  
For example, the client starts an FTP session on the Logical Server **FTP\_servers** (whose **Server** is defined as **FTP\_Group**, consisting of the servers **EastEnd**, **Trafalgar** and **Whitehall**, as shown in **FIGURE 8-2** on page 235).
- 2 FireWall-1 determines that the session is to be redirected to a particular server.  
For example, FireWall-1 determines, on the basis of the load balancing algorithm defined for the Logical Server **FTP\_Servers**, that **Trafalgar** will be the server for this session.
- 3 Using the Address Translation mechanism, FireWall-1 modifies the destination IP address of incoming packets.  
If a back connection is opened (for example, in FTP), the connection is correctly established between the server and the client automatically. The source IP address of reply packets is changed back to the Logical Server's IP address.

## Load Balancing Algorithms

The available load balancing algorithms are:

- 1 server load

### Logical Servers

FireWall-1 queries the servers to determine which is best able to handle the new connection. There must be a load measuring agent on the server.

#### 2 round trip

FireWall-1 uses PING to determine the round-trip times between the FireWall and each of the servers, and chooses the server with the shortest round trip time.

This method will not give optimum results for HTTP if some of the HTTP servers are not behind the FireWall, because it measures the round-trip time between the FireWall and the servers, and not between the client and the servers.

#### 3 round robin

FireWall-1 simply assigns the next server in the list.

#### 4 random

FireWall-1 assigns a server at random.

#### 5 domain

FireWall-1 assigns the "closest" server, based on domain names.

### Logical Servers

To implement the FireWall-1 Load Balancing feature, proceed as follows (the example is based on the configuration depicted in FIGURE 8-2 on page 235):

#### 1 Define a group network object consisting of all the servers that will be providing the given service.

For example, define a group network object **HTTP\_Group** that consists of Tower, Palace, BigBen and Louvre. There should be no other servers in the group.

#### 2 Define a network object of type Logical Server, and define its properties.

## Load Balancing

## 3 Define a Logical Server as in FIGURE 8-3.

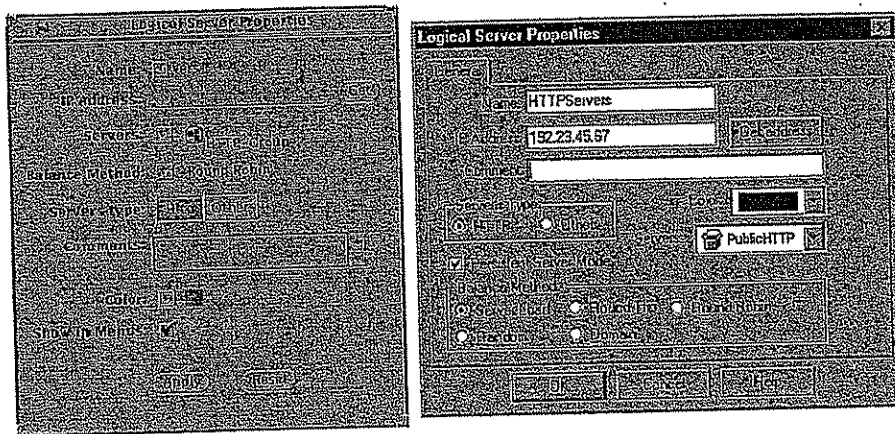


FIGURE 8-3 Logical Server Properties Window

**IP Address** must be an address for which communications are routed to or through the FireWall. This should be either the FireWall's address, or the address of a non-existing computer in the network behind the FireWall. This is the address that clients use to communicate with the Logical Server.

**Persistent Server Mode** — If this is checked, then once a client is connected to a physical server, the client will continue to connect to that server for the duration of the session.

**Servers** is HTTP\_Group.

None of the network objects that belong to **Servers** may have the IP address listed under **IP Address**.

**Balance Method** is one of the algorithms described under "Load Balancing Algorithms" on page 236.

**Servers Type** is HTTP.

This parameter determines how the redirection is performed. For further information, see "How Load Balancing Works" on page 235. Note that even for a Logical Server consisting of HTTP servers, **Servers Type** can be Others.

## Rule Base

- 4 Add the appropriate rules to the Rule Base, for example, the one in FIGURE 8-4.

No.	Source	Destination	Service	Action	Track	Install On
1	Any	HTTP_Servers	HTTP	Accept	Long	Gateways
2	Any	HTTP_Group	HTTP	User Auth	Long	Gateways
3	Any	Any	Any	reject	Long	Gateways

FIGURE 8-4 Using Logical Servers in a Rule

TABLE 8-1 Explanation of Rule Base

Rule No.	Explanation
1	balances the load for connections to the Logical Server HTTP_Servers
2	specifies that HTTP connections to HTTP_Group be User Authenticated (could also be Accept)
3	rejects and logs all other communications

## Rule Base

### Using HTTP Logical Servers in a Rule

When an HTTP Logical Server is the **Destination** in a rule, the rule's **Action** refers to the connection between the FireWall and the client (the connection that serves to redirect the client to the proper server), and must be either **Accept** or **Encrypt**. There must be a different rule that allows the connection between the client and the server. That rule can specify another action, for example, **User Authentication**.

The rule specifying the Logical Server as **Destination** must come before the rule specifying the physical servers as **Destination**.

In the configuration depicted in FIGURE 8-2 on page 235, HTTP connections to the HTTP servers behind the FireWall will be User Authenticated (in accordance with the second rule in FIGURE 8-4 on page 239), but HTTP connections to Louvre will not be User Authenticated, because they do not pass through the FireWall, even though they were enabled by the FireWall.

### Using non-HTTP Logical Servers in a Rule

There are no special considerations for using non-HTTP Logical Servers in a rule. One rule, with the Logical Server as **Destination**, is sufficient.

## Load Measuring

CheckPoint provides a sample load measuring agent application for installation on servers that are not FireWalled, as well as an API for users who wish to write their own agents.



### Connection Accounting

The load measuring agent is a service running on the port number specified in the **Load Agents Port** property (in the **Miscellaneous** tab of the **Properties Setup** window in the Windows GUI or in the **Control Properties/Miscellaneous** window in the OpenLook GUI) and returns information about the server's load to FireWall-1. All the load measuring agents in a configuration must use the same port number.

The load measuring agent measures the load at the interval specified by the **Load Measurement Interval** property, also defined in the **Miscellaneous** tab of the **Properties Setup** window in the Windows GUI or in the **Control Properties/Miscellaneous** window in the OpenLook GUI.

For example, in the configuration depicted in FIGURE 8-2 on page 235, the server Louvre is not FireWalled, so the only way for FireWall-1 on London to know what Louvre's load is (and to what extent Louvre is able to handle additional clients), is for Louvre's system administrator to install a FireWall-1 compatible load measuring agent on Louvre.

### Connection Accounting

You can generate accounting log entries by choosing **Accounting** in a rule's **Track** field. The accounting log entries show the start and end times of each connection, and the number of bytes transferred.

For additional information, see Chapter 11, "Log Viewer" of *Managing FireWall-1 Using the Windows GUI* or *Managing FireWall-1 Using the OpenLook GUI*.

### Active Connections

You can view the Active connections at any moment from the Log Viewer.

For additional information, see Chapter 11, "Log Viewer" of *Managing FireWall-1 Using the Windows GUI* or *Managing FireWall-1 Using the OpenLook GUI*.

CHAPTER **9**

# SNMP and Network Management Tools

## In This Chapter

<i>Overview</i>	<i>page 241</i>
<i>FireWall-1 HP OpenView Extension</i>	<i>page 243</i>
<i>FireWall MIB Source</i>	<i>page 248</i>

## Overview

### FireWall-1 SNMP Agent (daemon)

FireWall-1 includes a full SNMP V2 agent with both V1 (r/w community) and V2 security features. Furthermore, FireWall-1 pre-defines the SNMP and SNMP-read services so you can further protect your SNMP agent by restricting read and write access to it.

The FireWall-1 SNMP daemon (snmpd) is compatible with network management software such as HP OpenView. In addition, the FireWall-1 SNMP daemon is compatible with RFCs 1155, 1156, and 1157. The Management Information Base (MIB) in `$FWDIR/lib/snmp/mib.txt` supports RFCs 1155-1213. The SNMP daemon also provides FireWall-1 specific variables.

Installing the FireWall-1 SNMP daemon is optional. FireWall-1 does not require that any SNMP daemon be installed.

### Ports to Which the FireWall-1 SNMP daemon binds

FireWall-1's SNMP daemon is started when the FireWall-1 system is started (fwstart) and is stopped when FireWall-1 is stopped (fwstop).

241

## Overview

The FireWall-1 SNMP daemon tries to bind to the standard SNMP port (161) and also to port 260. If it fails to bind to port 161 (presumably because another SNMP daemon is already bound to that port), then it binds only to port 260 and passes on all non-FireWall-1 specific SNMP queries to the SNMP daemon on port 161.

If there is no daemon bound to port 161, FireWall-1's daemon binds to both ports (161 and 260). This allows all clients to use FireWall-1's daemon. If another SNMP daemon attempts to bind to port 161 after FireWall-1's SNMP daemon is started, the other daemon will fail to bind to the port. In the event that it is important for you to use an SNMP daemon other than FireWall-1's, start it before you start FireWall-1.

Trap alert as well as status reports can be sent to SNMP-based management software.

Under Windows NT, the FireWall-1 SNMP agent is an extension of the NT SNMP agent. If you have not installed the standard NT SNMP agent, you will not be able to use the FireWall-1 SNMP agent.

## Initial Communities ("Keys")

The initial SNMP communities ("keys") are public and private for read and write, respectively. To change these keys, edit `$FWDIR/conf/snmp.C`, and set the values for the read and write attributes for `:snmp_community`.

## Firewall-1 MIB

The variable definitions for Firewall-1's SNMP daemon are located in the files `$FWDIR/lib/snmp/chkpnt.mib`. This file can be used to incorporate the Check Point MIB into any MIB browser or network management system. All of Firewall-1's SNMP variables are located in the subtree `1.3.6.1.4.1.2620.1.1` (also known as `enterprises.checkpoint.products.fw`).



**Note** – Previous versions of FireWall-1 used enterprise ID 1919 for Check Point private MIB. FireWall-1 version 4.0 uses 2620 — the official Check Point enterprise ID (1.3.6.1.4.1.2620), as the prefix for all Check Point specific MIB variables. SNMP traps also use the updated enterprise ID.

## FireWall-1 SNMP Agent (daemon)

TABLE 9-1 lists the variables that are unique to FireWall-1, and unless otherwise noted, are strings of up to 256 bytes.

TABLE 9-1 FireWall-1 MIB Variables

Variable	Meaning
fwModuleState	the state of the Inspection Module
fwFilterName	the name of the currently loaded Security Policy
fwFilterDate	the date the Security Policy was installed
fwAccepted	the number of packets accepted by the Inspection Module since the last Security Policy was installed (an integer)
fwRejected	the number of packets rejected by the Inspection Module since the last Security Policy install (an integer)
fwDropped	the number of packets dropped by the Inspection Module since the last Security Policy install (an integer)
fwLogged	the number of packets logged by the Inspection Module since the last Security Policy was installed (an integer)
fwMajor	the FireWall-1 major release number (for example, for FireWall-1 Version 4.0 this is 4) — an integer
fwMinor	the FireWall-1 minor release number (for example, for FireWall-1 Version 4.0 this is "0") — an integer
fwProduct	the FireWall-1 product
fwEvent	the last SNMP trap sent by FireWall-1

The source of the FireWall-1 MIB is listed in "FireWall MIB Source" on page 248.

## FireWall-1 HP OpenView Extension

HP OpenView Network Node Manager displays hierarchical maps of the network topology. The FireWall-1 extension provides information on FireWalled objects in the network. The extension enables administrators to:

- display FireWalled objects within the context of the entire network
- specify network objects and devices as FireWalled objects
- open the FireWall-1 Log, Security Policy and System Status views

To enable this feature, the machine running the OpenView Network Node Manager session must have a FireWall-1 GUI client installed. The GUI client must be permitted by the FireWall-1 Management Server, and you must be one of the allowed administrators.

- display connection statistics and SNMP alert information for FireWalls
- access Check Point MIB data

## FireWall-1 HP OpenView Extension

**Installing the FireWall-1 HP OpenView Extension**

TABLE 9-2 lists the minimum hardware, operating system, and software requirements for installing the FireWall-1 Extension for HP OpenView Network Node Manager.

TABLE 9-2 Minimum Requirements

<b>Platforms</b>	HP EA-RISC 700/800, Sun SPARC-based systems
<b>Operating System</b>	HP-UX 10.x, Solaris 2.3 and higher
<b>Software</b>	FireWall-1 X/Motif GUI Client HP OpenView Network Node Manager version 4.1x

For hardware and software requirements of HP OpenView Network Node Manager, consult the HP documentation.

See TABLE 2-2 on page 37 of *Getting Started with FireWall-1* for information about the location of the FireWall-1 HP OpenView Extension on the FireWall-1 CD-ROM.

You can install the FireWall-1 HP OpenView Extension either directly from the CD-ROM, or you can recursively copy the installation files from the CD-ROM to a directory on your disk and install from there.

**▼ To install the FireWall-1 HP OpenView Extension (Solaris2)**

- 1 Become superuser.
- 2 Change to the directory in which the installation files are located (either on the CD-ROM or on the hard disk).
- 3 Enter the following command to install the FireWall-1 HP OpenView Extension:

```
hostname# pkgadd -d .
```

- 4 pkgadd presents a list of packages, and asks you to choose one to install.  
Specify the FireWall-1 HP OpenView Extension by entering either its name or its number in the list.

**▼ To install the FireWall-1 HP OpenView Extension (HP-UX)**

See "Special Notes for HP-UX 10" on page 56 of *Getting Started with FireWall-1* for information about the Rock Ridge format in which the FireWall-1 CD is written and HP-UX.

If you encounter a problem with the depth of the CD-ROM directories, use the files in `hpux/TarFiles`.

- 1 Become superuser.
- 2 Copy the installation files to the `/tmp` directory.

## Uninstalling the FireWall-1 HP OpenView Extension

- 3 If the /tmp directory has not been registered as an installation directory, enter the following command to register it.

```
hostname# swreg -l depot -x select_local=true /tmp
```

For information about the swreg command, refer to the HP-UX documentation.

- 4 Enter the following command to install the FireWall-1 HP OpenView Extension:

```
hostname# swinstall &
```

- 5 The SD Install - Software Selection window is displayed, and then the Specify Source window is displayed on top of it.  
For information about the swinstall command, refer to the HP-UX documentation.
- 6 Click on Source Depot Path.
- 7 In the Depot Path window, select the directory in which the installation files are located.
- 8 Click on OK to close the Depot Path window.
- 9 Click on OK to close the Specify Source window.
- 10 In the SD Install - Software Selection window, select FireWall-1 HP OpenView Extension.
- 11 From the Actions menu, select Install (analysis).
- 12 When the analysis phase completes, click on OK.
- 13 When the installation phase completes, click on Done.
- 14 From the File menu, select Exit.

## Uninstalling the FireWall-1 HP OpenView Extension

## ▼ To uninstall the FireWall-1 HP OpenView Extension (Solaris2)

Use the pkgrm application to uninstall the FireWall-1 HP OpenView Extension.



## FireWall-1 HP OpenView Extension

## ▼ To uninstall the FireWall-1 HP OpenView Extension (HP-UX)

- 1 Become superuser.
- 2 Type the following command:

```
hostname# swremove FWMap
```

**Viewing FireWalled Objects****Network Submap**

HP OpenView Windows displays a hierarchical map of all the devices, systems and FireWalls in the network. FireWalled objects are represented in a network submap by a FireWall icon.

**FireWalls Window**

The FireWalls window displays only the FireWalled objects in the network. To open the FireWalls window, double-click on the FireWalls icon in the root submap. To access the root submap, click on the **Root Submap** icon on the Open View toolbar.

HP OpenView identifies as FireWalled objects only those objects running the FireWall-1 SNMP daemon.

The FireWall discovery takes place when HP OpenView Windows (ovw) is started and whenever a new device is added to the network. If you start FireWall-1 after the FireWall discovery, the object will not be identified as FireWalled unless specifically queried (see "Query Selected" below).

If HP OpenView discovers a FireWalled object with the FireWall-1 SNMP daemon on port 260, it changes its default SNMP port for that object to 260.

## Viewing FireWalled Objects

**FireWall Menu**

The FireWall menu appears in the menu bar of the submap window.

**TABLE 9-3** FireWall Menu Commands

Menu Entry	Description										
Query Selected	Performs discovery on the selected objects.										
Set as FireWall	Sets a network object as a FireWall. This option is enabled only if a FireWall Module was not detected on the selected object.										
Unset as FireWall	Clears FireWall settings from the selected object. This option is enabled only if the object was manually set as a FireWall.										
FireWall-1	<p>This entry displays a sub-menu with the following options:</p> <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td>Log View</td><td>Opens the Log View</td></tr> <tr> <td>Security Policy</td><td>Opens the Security Policy</td></tr> <tr> <td>System Status</td><td>Opens the System Status View</td></tr> <tr> <td>Statistics</td><td>Displays a graph indicating the number of frames accepted, logged, dropped and rejected for the selected FireWall.</td></tr> </table> <p>You can also access the above options by right-clicking on a FireWalled object.</p> <p><b>Note:</b> In order to open the FireWall-1 GUI, the machine running the current OpenView Windows session must have a FireWall-1 GUI client installed. In addition, the GUI client must be permitted by the FireWall's Management Server and you must be one of the allowed administrators.</p>	Option	Description	Log View	Opens the Log View	Security Policy	Opens the Security Policy	System Status	Opens the System Status View	Statistics	Displays a graph indicating the number of frames accepted, logged, dropped and rejected for the selected FireWall.
Option	Description										
Log View	Opens the Log View										
Security Policy	Opens the Security Policy										
System Status	Opens the System Status View										
Statistics	Displays a graph indicating the number of frames accepted, logged, dropped and rejected for the selected FireWall.										

**FireWall-1 Management Servers**

When you start one of the FireWall-1 GUI applications (Security Policy, Log Viewer or System Status), the applications runs against the FireWalled object's Management Server, which is not necessarily the same machine as the FireWalled object. If the FireWall Module and the Management Server are on different machines, then you must configure the FireWalled object as follows:

- 1 Select the FireWalled object.
- 2 From the Edit menu, choose **Describe/Modify Object**.
- 3 In the **Object Description** dialog box, choose **FireWall-1 Management**. The **FireWall-1 Management** dialog box displays the host name of the Management Server.
- 4 Enter the name of the Management Server and click on **OK**.

Specify the correct host name or IP address.

## FireWall MIB Source

**FireWall-1 SNMP Traps**

The **Application Alert Events** browser displays a log of SNMP traps. All FireWall-1 SNMP traps appear in the **Application Alert Events** browser.

**Note** – You must first direct FireWall-1 SNMP traps to the host running OpenView using the `snmp_trap` command. For more information see “snmp\_trap” on page 284.

**Check Point MIB Data**

The Check Point MIB is accessible through the Network Node Manager SNMP MIB browser.

To access the Check Point MIB, proceed as follows:

- 1 Choose **SNMP MIB Browser** from the **Misc** menu. The **Browse MIB** dialog box is displayed.
- 2 Navigate to the Check Point MIB, which is located under the **Enterprises** subtree.

**FireWall MIB Source**

This section presents the source code for the FireWall-1 MIB (in `$FWDIR/lib/snmp/chkpnt.mib`).

```
CHECKPOINT-MIB DEFINITIONS ::= BEGIN

-- SUBTREE: 1.3.6.1.4.1.2620.1.1
-- iso.org.dod.internet.private.enterprises.checkpoint.products.fw

IMPORTS
    enterprises
        FROM RFC1155-SMI
    TRAP-TYPE
        FROM RFC-1215
    OBJECT-TYPE
        FROM RFC-1212;

-- textual conventions

DisplayString ::=
    OCTET STRING
-- This data type is used to model textual information taken
-- from the NVT ASCII character set. By convention, objects
-- with this syntax are declared as having
--
--     SIZE (0..255)

checkpoint OBJECT IDENTIFIER ::= { enterprises 2620 }
```

## Viewing FireWalled Objects

```

products OBJECT IDENTIFIER ::= { checkpoint 1 }
fw        OBJECT IDENTIFIER ::= { products 1 }

-- the FW group
-- Overall statistics and state
-- To be added a table of statistics by interfaces.

fwModuleState OBJECT-TYPE
    SYNTAX  DisplayString (SIZE (0..255))
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
        "The state of the fw module."
    ::= { fw 1 }

fwFilterName OBJECT-TYPE
    SYNTAX  DisplayString (SIZE (0..255))
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
        "The name of the loaded filter."
    ::= { fw 2 }

fwFilterDate OBJECT-TYPE
    SYNTAX  DisplayString (SIZE (0..255))
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
        "When was the filter installed (STRING!)"
    ::= { fw 3 }

fwAccepted OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
        "The number of accepted packets."
    ::= { fw 4 }

fwRejected OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
        "The number of rejected packets."
    ::= { fw 5 }

fwDropped OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION

```

## FireWall MIB Source

```

        "The number of dropped packets."
        ::= { fw 6 }

fwLogged OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
        "The number of logged packets."
        ::= { fw 7 }

fwMajor OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
        "FireWall-1 Major Version."
        ::= { fw 8 }

fwMinor OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
        "FireWall-1 Minor Version."
        ::= { fw 9 }

fwProduct OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
        "FireWall-1 Product."
        ::= { fw 10 }

fwEvent OBJECT-TYPE
    SYNTAX  DisplayString (SIZE (0..255))
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
        "A string containing the last snmp trap sent via fw"
        ::= { fw 11 }

Note - The following comment lines are a description of the MIB used by the SNMP traps generated by
FireWall-1.
--      fwTrap TRAP-TYPE
--          ENTERPRISE fw
--          VARIABLES { fwEvent }
--          DESCRIPTION

```

Viewing FireWalled Objects

```
--      "FireWall-1 SNMP trap"
--      ::= 0
END
```



FireWall MIB Source

252 FireWall-1 Architecture and Administration • September 1998

CHAPTER **10**

# Command Line Interface

## In This Chapter

<i>Unix-NT Syntax Differences</i>	<i>page 253</i>
<i>Setup</i>	<i>page 254</i>
<i>Control</i>	<i>page 257</i>
<i>Monitor</i>	<i>page 264</i>
<i>Utilities</i>	<i>page 273</i>

## Unix-NT Syntax Differences

The command line syntax presented here is the Unix syntax. Differences between the Unix and NT command line syntax are described in TABLE 10-1.

**TABLE 10-1** Unix-NT Syntax Differences

Unix	NT
/ in file names	\ in file names
fw m	fw m (space after fw)
fw d	fw d (space after fw)

### Setup

## Setup

<i>fwconfig</i>	page 254
<i>fwstart</i>	page 256
<i>fwstop</i>	page 256
<i>fw</i>	page 256

## fwconfig

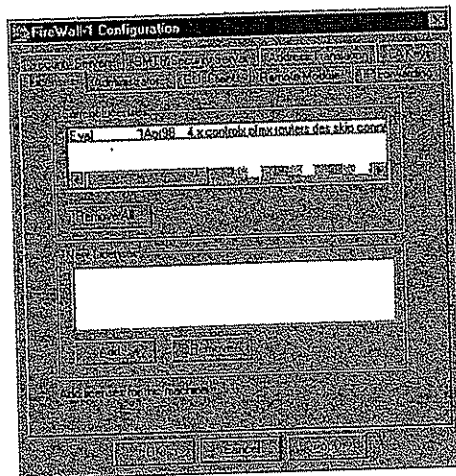
### Syntax

fwconfig

Windows NT

fwconfig reconfigures an existing FireWall-1 installation.

In Windows NT, the reconfiguration application is a GUI application that displays all the configuration windows from the FireWall-1 installation as tabs in the same window (FIGURE 10-1).



**FIGURE 10-1** FireWall-1 Configuration window

To reconfigure an option, click on the appropriate tab and modify the fields as required. Click on **OK** to apply the changes.

The tabs and their fields are described in "Configuration" on page 45 of *Getting Started with FireWall-1*.

## Unix

fwconfig displays the following screen (FIGURE 10-2). Choose the configuration options you wish to reconfigure.

```

Welcome to FireWall-1 Configuration Program.
=====
This program will let you re-configure your FireWall-1
configuration.

Configuration Options:
-----
(1) Licenses
(2) Administrators
(3) GUI clients
(4) Remote Modules
(5) Security Servers
(6) SMTP Server
(7) SNMP Extension
(8) Groups
(9) IP Forwarding
(10) Default Filter
(11) Random Pool
(12) CA Keys

(13) Exit

Enter your choice (1-13) :
Thank You...

```

**FIGURE 10-2** fwconfig Configuration Options

TABLE 10-2 lists the reconfiguration options.

**TABLE 10-2** fwconfig Configuration Options

option	description	see also ...
licenses	Update FireWall-1 licenses.	"fw putlic" on page 262
administrators	Update the list of administrators, users who are authorized to connect to a Management Server through the GUI.	Chapter 7, "Management Server"
GUI clients	Update the list of GUI Clients, machines from which administrators are authorized to connect to a Management Server through the GUI.	Chapter 7, "Management Server"

## Setup

TABLE 10-2 fwconfig Configuration Options

option	description	see also ...
remote modules	Update the list of remote FireWall and Inspection Modules managed by a Management Module.	Chapter 7, "Management Server"
Security Servers	Configure the Security Servers.	Chapter 2, "Security Servers"
SMTP Server	Configure the SMTP Security Server.	"SMTP Security Server Configuration" on page 111"
SNMP Extension	Configure the SNMP Extension.	Chapter 9, "SNMP and Network Management Tools"
Groups	Update the list of Unix groups authorized to run FireWall-1.	
IP Forwarding	Configure IP Forwarding on the gateway.	"Enabling and Disabling IP Forwarding" on page 276
default filter	Configure the default Security Policy.	"Default Security Policy" on page 319
random pool	Configure RSA keys.	<i>Virtual Private Networking with FireWall-1</i>
CA keys	Configure Certificate Authority keys.	<i>Virtual Private Networking with FireWall-1</i>

**fwstart**

fwstart loads the FireWall-1 FireWall Module, starts the FireWall-1 daemon (fwd), the FireWall-1 SNMP daemon (snmpd) and the authentication daemons, and starts fwm, the Management Server (see Chapter 7, "Management Server").

**fwstop**

fwstop kills the FireWall-1 daemon (fwd) and the Management Server (fwm), the FireWall-1 SNMP daemon (snmpd), and the authentication daemons, and then unloads the FireWall Module.

**fw**

The fw program is used to manage the system. Its specific action is determined by the first command line argument, as described in the following sections. Commands may have a subject (target). There are three options to specify the targets (see "Targets" on page 257). If more than one is used, the command will execute on the combination of targets.

For each option, it is sufficient to type the first character. Commands and options are described below.

If the first argument is "-d" then debug information is generated as fw runs.

## Control

<i>fw load</i>	<i>page 257</i>
<i>fw unload</i>	<i>page 259</i>
<i>fw fetch</i>	<i>page 259</i>
<i>fw logswitch</i>	<i>page 260</i>
<i>fw putkey</i>	<i>page 261</i>
<i>fw putlic</i>	<i>page 262</i>
<i>fw dbload</i>	<i>page 264</i>

### fw load

*fw load* compiles and install a Security Policy to the target's FireWall Modules.

#### Syntax

```
fw load [-all | -conf confile] [filter-file | rule-base] targets
```

*fw load* compiles and installs an Inspection Script (\*.pf) file into the targets' FireWall Modules. It converts a Rule Base (\*.w) file created by the GUI into an Inspection Script (\*.pf) file and perform the above operations. For more information, see "fw gen" on page 278.

If no target is specified, the Inspection Code is installed on the local host.

#### Targets

parameter	meaning
-conf confile	The command is executed on targets specified in confile. Each line in confile has the syntax of a target in a target list (see "Targets" on page 257).
-all	The command is executed on all targets specified in the default system configuration file (\$FWDIR/conf/sys.conf).
targets	The command is executed on the specific named target. See below for an explanation of the syntax of this argument. The dot (.) and the at-sign (@) are part of the format; spaces around them are not allowed.



## Control

## Formats

```
interface.direction@host
host
interface.direction
```

## Examples

```
le0.in@host1
all@host2
host3
all.out
all.all
```

## Explanation

parameter	meaning
interface	name of an interface on the target host. If all is specified, all configured interfaces on the target host will be loaded. examples: le0; lo0; all.
direction	one of: in, out, or all. The reference point for the direction is the target host.
host	target host is specified using the host's name (the name returned by the hostname command) or its IP address.
all	has different meaning according to its place. It may specify: both directions, all interfaces or both directions on all interfaces.

If host is not specified, localhost is assumed. If only host is specified, all is assumed (meaning both directions on all interfaces).

Several targets may be specified in various formats. Command-line separators are subject to the rules of the shell (spaces and tabs are the most common separators).

The format of configuration files is identical to the format of targets. In configuration files, the following separators may be used: spaces, tabs, comma, or new line.

**Note** – The scope of a set of rules in a Rule Base and the targets of a Rule Base installation are not the same. The system will install the entire Rule Base on the designated targets. However, only the rules whose scope includes the target system will actually be enforced on a target.

Loading any interface of a target host first completely unloads it. Hence, some interfaces on a target host might be left unloaded (if the new Rule Base or compiled FireWall Module does not contain a rule for them).

To protect a target, you must load a Rule Base that contains rules whose scope matches the target. If none of the rules are enforced on the target, then all traffic through the target is blocked.

#### Examples

```
fw load my_rules.W
fw load gateway.pf gateway1
fw load -all complex_rules.pf
```

### fw unload

fw unload uninstalls the currently loaded Inspection Code from selected targets.

#### Syntax

```
fw unload [-all | -conf confile] targets
```

#### Examples

```
fw unload gateway1
fw unload -a
```

### fw fetch

fw fetch fetches the Inspection Code that was last installed on the local host. You must specify the Master where the Inspection Code is found. Use "localhost" in case there is no Master or if the Master is down. You may specify a list of Masters, which will be searched in the order listed.

#### Syntax

```
fw fetch targets
```

#### Examples

```
fw fetch gateway1
```

Control

**fw logswitch**

fw logswitch creates a new Log File. The current Log File is closed and renamed \$FWDIR/log/fw.logcurrent date, and a new Log File with the default name (\$FWDIR/log/fw.log) is created. Old Log Files are located in the same directory. You must have the appropriate file privileges to run fw logswitch.

In addition, a Management Station can use fw logswitch to switch a Log File on a remote machine and transfer the Log File to the Management Station. For information on how to direct logging to a specific machine, see "Redirecting Logging to Another Master" on page 327.

Syntax

```
fw logswitch [-h target] [+|-|""old_log]
```

Explanation

parameter	meaning
target	The resolvable name or IP address of the remote machine (running either a FireWall Module or a Management Module) on which the Log File is located. The Management Station (on which the fw logswitch command is executed) must be defined as one of target's Management Stations. In addition, you must perform fw putkey to establish a control channel between the Management Station and target. For information about establishing control channels, see "How Can Distributed Configurations Be Managed?" on page 345.
+	The Log File is transferred from target to the Management Station. The transferred Log File is compressed and encrypted. The name of the copied Log File on the Management Station is prefixed by target (see TABLE 10-3 for details). This parameter is ignored if target is not specified. There should be no white space between this parameter and the next one.
-	The same as +, but the Log File is deleted on target.
""	Delete the current Log File (on target if specified; otherwise on the Management Station).
old_log	The new name of the old Log File.

TABLE 10-3 lists the files created in the \$FWDIR/log directory on both target and the Management Station when the + or - parameters are specified. Note that if "-" is

specified, the Log File on target is deleted rather than renamed.

TABLE 10-3 File names

	old_log specified	old_log not specified
target specified	On target, the old Log File is renamed to old_log. On the Management Station, the copied file will have the same name, but prefixed by target's name. For example, the command <code>fw logswitch -h venus +xyz</code> creates a file named <code>venus.xyz</code> on the Management Station.	On target, the new name is current date. For example, <code>04Feb98-10:04:20</code> in Unix and <code>04Feb98-100420</code> in NT. On the Management Station, the copied file will have the same name, but prefixed by target's name ( <code>target.04Feb98-10:04:20</code> in Unix and <code>target.04Feb98-100420</code> in NT.)
target not specified	On the Management Station, the old Log File is renamed to old_log.	On the Management Station, the old Log File is renamed to current date. (see above).

If either the Management Station or target is an NT machine, the files will be created using the NT naming convention (see TABLE 10-3 above).

#### Example

The following command creates a new Log File and moves (renames) the old Log File to old\_log.

```
fw logswitch old_log
```

See also "How can I switch my Log File on a periodic basis?" on page 363.

#### fw putkey

`fw putkey` installs a FireWall-1 authentication password on a host, thus enabling control connections between the host on which the `fw putkey` command is run and a second host.

#### Syntax

```
fw putkey <target> [-no_opsec] [-opsec] [-p password]
               [-k num] [-n name]
```

This password is used to authenticate internal communications between FireWall Modules and between a FireWall Module and its Management Center. The password is used to authenticate the control channel the first time communication is established. For a detailed example of how `fw putkey` is used, see "How Can Distributed Configurations Be Managed?" on page 345.

**Control**

The password can be entered on the command line (using the `-p` argument), or interactively.

**Explanation**

parameter	meaning
target	The IP address or the resolvable name of the other host on which you are installing the key (password). This should be the IP address of the interface "closest" to the host on which the command is run. If it is not, you will get error messages such as the following: "/fwd: Authentication with <i>hostname</i> for command sync failed"
-no_opsec	Only FireWall-1 control connections are enabled.
-opsec	Only OPSEC control connections are enabled.
-k num	The length of the first S/Key password chain for fwal authentication. The default is 7. When less than 5 passwords remain, the hosts renegotiate a chain of length 100, based on a long random secret key. The relatively small default value ensures that the first chain, based on a short password entered by the user, is exhausted relatively quickly.
-n name	The IP address (in dot notation) to use in identifying this host to the other host, instead of the resolution of the <i>hostname</i> command.
-p password	The key (password). You will be prompted for this if you do not enter it in the command line.

If neither `-opsec` nor `-no_opsec` is specified, then both FireWall-1 and OPSEC connections are enabled.

**fw putlic**

`fw putlic` installs a FireWall-1 license on a host.

You can also install licenses with the `fwconfig` command (see "fwconfig" on page 254).

After installing license, it's best to do the following:

- 1 Stop the FireWall Module (`fwstop`).
- 2 Start the FireWall Module (`fwstart`).
- 3 Determine the current licenses with the `fw printlic -k` command (see "fw printlic" on page 268).

## Syntax

```
fw putlic [-overwrite]
          [-check-only] [-check-one] [-f licensefile]
          [-n netmask] [-kernelonly]
hostname|ip-addr|hostid|eval
k1-k2-k3 features
```

## Explanation

parameter	meaning										
-l overwrite	overwrite (delete) all existing licenses with the new license										
-check-only	verify the license										
-check-one											
-f licensefile	the name of the file with the license text										
-kernelonly	copy the user level license to the kernel — takes no parameters										
hostname	the host's name (the name returned by the hostname command)										
ip-addr	the host's IP address										
hostid	<table> <tr> <th>platform</th><th>type</th></tr> <tr> <td>Sun OS4 and Solaris2</td><td>the response to the hostid command (beginning with 0x)</td></tr> <tr> <td>HP-UX</td><td>the response to the uname -i command (beginning with 0d)</td></tr> <tr> <td>AIX</td><td>the response to the uname -l command (beginning with 0d), or the response to the uname -m command (beginning and ending with 00)</td></tr> <tr> <td>NT</td><td>IP address of the external interface (in dot notation); last part cannot be 0 or 255</td></tr> </table>	platform	type	Sun OS4 and Solaris2	the response to the hostid command (beginning with 0x)	HP-UX	the response to the uname -i command (beginning with 0d)	AIX	the response to the uname -l command (beginning with 0d), or the response to the uname -m command (beginning and ending with 00)	NT	IP address of the external interface (in dot notation); last part cannot be 0 or 255
platform	type										
Sun OS4 and Solaris2	the response to the hostid command (beginning with 0x)										
HP-UX	the response to the uname -i command (beginning with 0d)										
AIX	the response to the uname -l command (beginning with 0d), or the response to the uname -m command (beginning and ending with 00)										
NT	IP address of the external interface (in dot notation); last part cannot be 0 or 255										
eval	evaluation license										
k1-k2-k3	the license										
features	license features										

## Example

## Typing:

```
fw putlic eval 2f540abb-d3bcb001-7e54513e std routers
```



**Monitor**

produces output similar to the following:

Type	Expiration	Features
Eval	1Mar95	std routers
License file updated		
Putting license in /etc/fw/modules/fwmod.XXX.o		

**fw dbload**

fw dbload downloads the user database and network objects information (for example, encryption keys) to selected targets. If no target is specified, then the database is downloaded to localhost.

Syntax

```
fw dbload [targets]
```

**Monitor**

<i>fw stat</i>	<i>page 264</i>
<i>fw lichosts</i>	<i>page 265</i>
<i>fw log</i>	<i>page 265</i>
<i>fw logexport</i>	<i>page 266</i>
<i>fw ver</i>	<i>page 267</i>
<i>fw printlic</i>	<i>page 268</i>
<i>fw sam</i>	<i>page 269</i>

**fw stat**

fw stat displays the status of target hosts in various formats.

Syntax

```
fw stat [-all | -conf confile] [-long] [-short]
        [-inactive] targets
```

The default format displays the following information for each host: host name, Rule Base (or FireWall Module) file name, date and time loaded, and the interface and direction loaded.

If no target is specified, the status of localhost is shown.

## Explanation

parameter	meaning
-short	use short format; for each direction and interface, displays: host name, direction, interface, Rule Base file name and loading date. This is the default format.
-long	use long format: in addition to short format, displays number of packets in each of the following categories: total, rejected, dropped, accepted, and logged.
-inactive	display status of inactive interfaces too (using the selected format). An inactive interface is an interface that had no packet flow since the last time the Rule Base was loaded on that interface.

## Examples

```
fw stat
fw stat -s -a
fw stat -l gateway1
```

**fw lichosts**

fw lichosts prints a list of hosts protected by the FireWall-1/n products.

The list of hosts is in the file \$FWDIR/database/fwd.h.

## Syntax

```
fw lichosts
```

**fw log**

fw log displays the content of Log Files.

## Syntax

```
fw log [-f[t]] [-c action] [-l] [-start time] [-end time]
      [-b stime etime]] [-h hostname] [log-file] [-n]
```

The default Log file is \$FWDIR/log/fw.log.

## Monitor

## Explanation

parameter	meaning
-f	After current display is completed, do not exit but continue to monitor the Log file and display it while it is being written.
-ft	Same as -f but do not display the current Log, only new events.
-c action	Display only events whose action is action, that is, accept, drop, reject, authorize, deauthorize, encrypt and decrypt. Control actions are always displayed.
-start time	Display only events that were logged after time. time may be a date, a time, or both. If date is omitted, then today's date is assumed.
-end time	Display only events that were logged before time. time may be a date, a time, or both.
-b stime etime	Display only events that were logged between stime and etime, each of which may be a date, a time, or both. If date is omitted, then today's date is assumed.
-l	Display the date for each record.
-h hostname	Display only log entries sent by the FireWalled machine hostname.
-n	don't perform DNS resolution of the IP addresses in the Log File (this option significantly speeds up the processing)
logfile	Use logfile instead of the default Log file.

## Examples

```
fw log
fw log | more
fw log -c reject
fw log -s Jan1
fw log -f -s 16:00
```

**fw logexport**

fw logexport exports the Log File to an ASCII file.

## Syntax

```
fw logexport [-d delimiter] [-i inputfile] [-o outputfile]
             [-r record_chunk_size] [-n]
```

## Explanation

parameter	meaning
-d delimiter	output fields will be separated by this character — default is comma (,)
-i inputfile	name of the input Log File
-o outputfile	name of the output ASCII file
-r record_chunk_size	determines how many records should be read (during a single access to the Log File) into the internal buffer for processing
-n	don't perform DNS resolution of the IP addresses in the Log File (this option significantly speeds the processing)

**fw ver**

fw ver displays the FireWall-1 version number. This is the version of the FireWall-1 daemon, the compiler and the Inspection Script generator (fw gen). The version of the GUI is displayed in the opening screen, and can be viewed at any time from the Help menu.

## Syntax

```
fw ver [ -k ]
```

## Explanation

parameter	meaning
-k	print the version number in the Kernel Module

Monitor

**fw printlic**

printlic prints details of the FireWall-1 license.

Syntax

```
fw printlic [-k]
```

Explanation

parameter	meaning
-k	print the license in the Kernel Module

Example

```
This is FireWall-1 Version 2.1a [VPN]
Type Expiration Features
Eval 15Jul96 pfm control routers
807dafa7 Never pfm control routers encryption [Invalid]
807dafa8 Never pfm control routers encryption
807dafa7 Never pfm control routers encryption
```

There are four licenses installed on this machine.

- The first is an evaluation license, which is valid for all computers, but only until July 15, 1996.
- The second is an invalid license, most likely because the user made some typing errors when entering license string.
- The third is a permanent license for hostid 807dafa8, which is perfectly valid, but irrelevant because the hostid is 807dafa7.
- Only the last license, which is unexpired, valid and for the correct hostid is actually used.

A valid license may still be irrelevant, because the date may be expired, or the hostid may be incorrect.

If several relevant licenses are installed, their features are ORed together.

**fw sam**

fw sam inhibits (blocks) connections to and from specific IP addresses without the need to change the Security Policy. The command is logged.

To "uninhibit" inhibited connections, execute fw sam again with the -C or -D parameters.

**Syntax**

```
fw sam [-v] [-s sam_server] [-f fwm] [-t timeout] [-C]
      [-n | -i | -I] mode <ip_address>
fw sam [-v] [-s sam_server] [-f fwm] [-t timeout] [-C]
      [-n | -i | -I] srv <source> <dest> <dport> <ip_protocol>
fw sam [-v] [-s sam_server] [-f fwm] [-t timeout] [-D]
```

**Explanation**

parameter	meaning						
sam_server	The IP address (in dot format) or the resolvable name of the FireWall that will enforce the command. The default is localhost, the machine on which the fw sam command is executed. See "Configuration Files" on page 270 for more information.						
fwm	Specifies the FireWall Modules on which to enforce the action. Can be the name of a FireWall object, group or one of the following (default is "All"): <table border="1"> <thead> <tr> <th>value</th><th>the action will be enforced on ...</th></tr> </thead> <tbody> <tr> <td>All</td><td>all the FireWalls which are defined as gateways or hosts on the machine on which the fw sam command is executed</td></tr> <tr> <td>Gateways</td><td>all the FireWalls which are defined as gateways on the machine on which the fw sam command is executed</td></tr> </tbody> </table> See "Configuration Files" on page 270 for more information.	value	the action will be enforced on ...	All	all the FireWalls which are defined as gateways or hosts on the machine on which the fw sam command is executed	Gateways	all the FireWalls which are defined as gateways on the machine on which the fw sam command is executed
value	the action will be enforced on ...						
All	all the FireWalls which are defined as gateways or hosts on the machine on which the fw sam command is executed						
Gateways	all the FireWalls which are defined as gateways on the machine on which the fw sam command is executed						
-v	Verbose mode — writes one message (describing whether the command was successful or not) to stderr for each FireWall on which the command is enforced.						
-n	Notify, that is, generate a long-format log entry and an alert when connections that match the specified services or IP addresses pass through the FireWall. This action does not inhibit or close connections.						



## Monitor

parameter	meaning										
timeout	Specifies the time period (in seconds) for which the action will be enforced. The default is forever.										
-i	Inhibit the specified connections (that is, do not allow new connections with the specified parameters). Each inhibited connection is logged (long format) and an alert is generated.										
-I	Inhibit the specified connections, and close all existing connections with the specified parameters. Each inhibited connection is logged (long format) and an alert is generated.										
-D	Cancel all inhibit (-i and -I) and notify (-n) commands.										
-C	Cancel the specified command (that is, inhibited connections with the specified parameters will no longer be inhibited). The parameters must match the ones in the original command.										
mode	One of the following: <table> <tr> <th>value</th><th>match</th></tr> <tr> <td>src</td><td>ip_address to the source IP address</td></tr> <tr> <td>dst</td><td>ip_address to the destination IP address</td></tr> <tr> <td>any</td><td>ip_address to either the source IP address or the destination IP address</td></tr> <tr> <td>srv</td><td>service</td></tr> </table>	value	match	src	ip_address to the source IP address	dst	ip_address to the destination IP address	any	ip_address to either the source IP address or the destination IP address	srv	service
value	match										
src	ip_address to the source IP address										
dst	ip_address to the destination IP address										
any	ip_address to either the source IP address or the destination IP address										
srv	service										
ip_address	IP address (in dot format or resolvable name) to be matched according to mode.										
source	source IP address (in dot format or resolvable name)										
dest	destination IP address (in dot format or resolvable name)										
dport	destination port (integer or name, for example, "telnet")										
ip_protocol	protocol (integer or name, for example, "tcp")										

## Configuration Files

There are two configuration files (in \$FWDIR/conf) that affect the functionality of the fw sam command:

## product.conf

This file (which you should not modify) has two parameters relevant to fw sam:

## ■ Management

When FireWall-1 is installed, this parameter is set to 1 on Management Modules (Servers) and to 0 on FireWall and Inspection Modules.

## ■ FireWall

When FireWall-1 is installed, this parameter is set to 0 on Management Modules (Servers) and to 1 on FireWall and Inspection Modules. On machines which are both Management Stations and FireWall Modules, this parameter is set to 1.

On a machine on which Management is 0, the `fw sam` command cannot perform remote actions (that is, it cannot inhibit connections through other machines).

On a machine on which FireWall is 0, the `fw sam` command cannot perform local actions (that is, it can inhibit connections *only* through other machines).

`fwopsec.conf`

The `sam_allowed_remote_requests` parameter (default value "no") determines whether the `fw sam` command on this machine can perform remote commands. To enable a FireWall Module to inhibit connections through other FireWalled Modules, set `sam_allowed_remote_requests` to "yes". Do not try to accomplish this by modifying `product.conf`.

Examples

The command:

```
fw sam -i src louvre -t 600
```

inhibits for 10 minutes all connections originating on louvre.

The command:

```
fw sam -C src louvre
```

is an invalid command because there is no timeout parameter. The cancel command's parameters must match the parameters of the command it is meant to cancel.

The command:

```
fw sam -C src louvre -t 60
```

is also an invalid command, because timeout is incorrect (it does not match timeout in the original command).

Monitor

The command:

```
fw sam -C any louvre -t 600
```

is also invalid, because mode does not match mode in the original command.

The command:

```
fw sam -C src louvre -t 600
```

cancels the command in the first example.

## Utilities

<i>fwciscoload</i>	<i>page 273</i>
<i>fw ctl</i>	<i>page 275</i>
<i>fw gen</i>	<i>page 278</i>
<i>fw kill</i>	<i>page 278</i>
<i>fwc</i>	<i>page 279</i>
<i>fwm</i>	<i>page 279</i>
<i>fwll</i>	<i>page 280</i>
<i>fw tab</i>	<i>page 283</i>
<i>fwxconf</i>	<i>page 283</i>
<i>snmp_trap</i>	<i>page 284</i>
<i>status_alert</i>	<i>page 284</i>
<i>fw converthosts</i>	<i>page 285</i>
<i>User Database - Importing and Exporting</i>	<i>page 285</i>

### fwciscoload

fwciscoload downloads a Security Policy to a Cisco router.

#### Syntax

If only a password and an enable-password are required, then the syntax is:

```
fwciscoload machine-name conf-file LoginPassword EnablePassword
```

#### Explanation

parameter	meaning
machine-name	router name
conf-file	Security Policy file (must be in \$FWDIR/conf)
LoginPassword	login password for the Cisco router
EnablePassword	enable password for the Cisco router

If the Cisco router uses the TACACS protocol, or if a user name is required in addition to the password and enable-password, then the syntax is:

```
fwciscoload machine-name conf-file UserName LoginPassword
EnableName EnablePassword
```

## Utilities

## Explanation

parameter	meaning
machine-name	router name
conf-file	Security Policy file (must be in \$FWDIR/conf)
UserName	user name
LoginPassword	login password for the Cisco router
EnableName	enable name
EnablePassword	enable password for the Cisco router

Each of the last four parameters can be XXX to indicate that it is unneeded, or PROMPT to indicate that the user should be prompted for the parameter. Use PROMPT when you do not want a password to appear on the command line, or if the password is not fixed (for example, with SecurID).

**Note** - XXX and PROMPT are case-insensitive and cannot be used as either name or password.

Alternatively, you can download the Security Policy using a TELNET-like interactive session. You should use this option when the enable-login is not covered by the above options. In this case, type:

```
fwciscoload machine-name conf-file -t
```

The interactive session will begin. Enter enable mode manually (type Ctrl-C to exit fwciscoload).

Type Ctrl-J to return to fwciscoload, which will then download the Security Policy and exit.

**Note** - If the TACACS authentication connection between the Cisco router and the TACACS server passes through a FireWalled machine, you must enable the connection in the Rule Base.

## Example

The command:

```
fwciscoload cis cis.cl XXX 1234 abcd PROMPT
```

downloads the policy file cis.cl (in \$FWDIR/conf) to the router cis.

- The login password is 1234.
- There is no UserName.
- EnableName is abcd.

- The user is prompted for a password (for example, a SecurID password).

### fw ctl

fw ctl sends control information to the FireWall-1 Kernel Module.

Syntax

```
fw ctl [ip_forwarding option] | pstat | install | uninstall
```

Explanation

parameter	meaning
ip_forwarding never	Specify that FireWall-1 does not control (and thus never changes) the status of IP Forwarding.
ip_forwarding always	Specify that FireWall-1 controls the status of IP Forwarding as described below.
ip_forwarding default	Specify that FireWall-1 controls the status of IP Forwarding only if IP Forwarding is disabled in the kernel. Otherwise, FireWall-1 does not control (and thus does not change) the status of IP Forwarding. This is the default setting.
pstat	Display FireWall-1 internal statistics.
install	Install the FireWall-1 kernel.
uninstall	Uninstall the FireWall-1 kernel.

IP Forwarding

```
fw ctl ip_forwarding always
```

When FireWall-1 controls the status of IP Forwarding, then FireWall-1 changes the status as follows:

- When FireWall-1 is stopped (fwstop), IP Forwarding is disabled.
- When FireWall-1 is started (fwstart), IP Forwarding is enabled.

This ensures that there is never a time (after FireWall-1 has been started for the first time) that the host is forwarding packets without the FireWall Module being loaded with a Security Policy.

It is recommended that IP Forwarding be disabled in the kernel. See "Enabling and Disabling IP Forwarding" on page 276 for instructions on how to do this. In this way, IP Forwarding will be never be enabled unless FireWall-1 is working, no matter which of the above options you have chosen.

In IBM AIX, IP Forwarding is by default disabled during boot, so it is not necessary to disable it in the kernel.



## Utilities

## Enabling and Disabling IP Forwarding

Solaris 2.x (source routed packets)

To turn off IP Forwarding and source routed packets, edit /etc/rc2.d/s69inet and change:

```
ndd -set /dev/ip ip_forwarding 1
```

to:

```
ndd -set /dev/ip ip_forwarding 0
nnd -set /dev/ip ip_forward_src_routed 0
```

For additional information, refer to the man pages for `ndd(1M)` and `ip(7)`.

## HP-UX 10

On HP-UX 10, the following commands can be put early in the `rc2.d` directory<sup>1</sup>, provided that `/usr` is mounted locally. In this case, you could put these statements in `/sbin/init.d/noipforward`:

```
#!/sbin/sh
PATH=/sbin:/usr/sbin:/usr/bin
export PATH
case "$1" in
  start_msg)
    echo "Turn IP-Forwarding OFF"
    ;;
  stop_msg)
    echo "(Not Turning IP-Forwarding on)"
    ;;
  'start')
    if [ -x /usr/bin/adb ]; then
      echo "ipforwarding/W 0" | adb -w /stand/vmunix
      /dev/kmem
    fi
    ;;
  esac
exit 0
```

1. The files in this directory are executed one after the other, in alphabetical sequence of their names.

Make sure `/sbin/init.d/noipforward` is executable and link it to `/sbin/rc2.d/S001noipforward`.

If `/usr` is not mounted locally, then put the above statements in a file that is executed after `/usr` is mounted.

To enable IP Forwarding, enter the following command:

```
echo "ipforwarding/W 1" | adb -w /stand/vmunix /dev/mem
```

#### Windows NT

- 1 When you install FireWall-1, check **Control IP Forwarding** in the **IP Forwarding** window (see FIGURE 2-18 on page 52 of *Getting Started with FireWall-1*).  
If you have already installed FireWall-1, reconfigure FireWall-1 using the FireWall-1 Configuration application. When you do so, the different configuration options will be displayed as different tabs in the Configuration window.

- 2 Enable the **IP Enable Routing** option in the **Advanced TCP/IP Configuration** window.

This window is accessible from the **TCP/IP Configuration** window in the Networks applet in the Control Panel.

- 3 Reboot the computer.

#### IBM AIX



**Warning** – The AIX default is for IP Forwarding to be off. If you enable IP Forwarding while FireWall-1 is not running, you will be exposing your network. Make sure that it is not turned on in one of the `.rc` scripts during boot. Turn it on (with the `no -o ipforwarding=1` command) in the `fwstart` script after FireWall-1 starts enforcing a Security Policy, and turn it off (with the `no -o ipforwarding=0` command) in the `fwstop` script just before FireWall-1 stops.

To enable IP Forwarding, enter the following command:

```
no -o ipforwarding=1
```

To disable IP Forwarding, enter the following command:

```
no -o ipforwarding=0
```

## Utilities

**fw gen**

`fw gen` generates an Inspection Script (\*.pf) file from a Rule Base (\*.W) file. The command takes a Rule Base file as an argument and the Inspection Script is printed to the standard output. Rule Base (\*.W) files are created by the Graphical User Interface, but you may edit them and use this command to generate Inspection Scripts (though this is *not* recommended).

## Syntax

```
fw gen <RuleBase_filename>
```

## Examples

```
fw gen $FWDIR/conf/default.W
fw gen $FWDIR/conf/corporate.W | more
fw gen $FWDIR/conf/corporate.W > /tmp/corporate.pf
```

**fw kill**

`fw kill` sends a signal to a FireWall-1 daemon.

## Syntax

```
fw kill [-t sig_no] proc-name
```

## Explanation

parameter	meaning
<code>[-t sig_no] proc-name</code>	If the file <code>\$FWDIR/log/&lt;proc-name&gt;.pid</code> exists, send <code>sig_no</code> to the pid given in the file. If no signal is specified, signal 15 (SIGTERM) is sent.

The FireWall-1 daemons and Security Servers write their pids to files in the log directory upon startup. These files are named `$FWDIR/log/<daemon_name>.pid`. For example, the file containing the pid of the FireWall-1 snmp daemon is `$FWDIR/log/snmpd.pid`.

**Examples**

```
fw kill snmpd
```

sends signal 15 to the FireWall-1 snmp daemon.

```
fw kill -t 1 snmpd
```

sends signal 1 to the FireWall-1 snmp daemon.

**fwc**

fwc is the FireWall-1 INSPECT language compiler. It compiles an Inspection Script (\*.pf) file but does not install it. You may use this command to see if your Inspection Scripts can be compiled, without actually installing them on FireWall Modules.

fwc takes an Inspection Script (\*.pf) file as an argument and produces several files: Inspection Code (\*.fc) file, FireWall Module tables (\*.ft) file, log format (\*.lg) file and \*.set, \*.db and \*.objects files. Those files are produced in the directory \$FWDIR/tmp.

**fwm**

fwm is the FireWall-1 Management Server in the Client/Server implementation of the Management Module, and is used for communicating with the GUI and adding, updating and removing administrators.

fwm must be running on the Management Server if you wish to use the GUI client on one of the client machines.

**Syntax**

```
fwm [-a name [-w{w|u|r|m}] [-s password] [-q] | -r name | -p | -g]
```

**Explanation**

parameter	meaning
-a name	add or update an administrator
-w	set access level as follows: w — Read/Write u — User Edit r — Read Only m — Monitor Only
-s password	set the administrator's password

## Utilities

parameter	meaning
-g	when adding an administrator, don't prompt for the administrator's password (useful for batch updates)
-r name	delete an administrator
-p	print a list of administrators
-g	convert the old *.W files to one unified rulebases.fws that is used by fwm

For more information about the FireWall-1 Management Server, see Chapter 7, "Management Server."

To add an administrator, type:

```
fwm -a
```

You will be prompted to type the user's name and password. You will be asked to confirm the password by typing it a second time.

To delete an administrator, type:

```
fwm -r
```

You will be prompted to type the user's name.

**fwell**

fwell manages Access Lists for Wellfleet (Bay Networks) routers.

## Syntax

```

fwell load rulebase-file [-s] [-u] [interface-name@]router-name
    [targets]
fwell unload [-s] [-u] [interface-name@]router-name targets
fwell stat    targets

```

## Explanation

parameter	meaning
load	loads the Access List to the router
unload	unloads the Access List
-s	generate summary output
stat	show statistics
-u	specifies list of interfaces

**Note** – When loading a Rule Base to a router, all the router's interfaces are first unloaded. If the -u parameter is specified, then the virtual router's interfaces are unloaded. If the -u parameter is not specified, then the real router's interfaces are unloaded.

For example, the command `fwell stat well` produces output similar to the following:

CIRCUIT	IF	FILTERDATE
E21	-	-
S21	192.114.50.33	d423Mar95 10:34:13
S22	-	-

## Individual Interface Loading for Bay Routers (Wellfleet)

Rather than loading (or unloading) the Security Policy (Access Lists) to (or from) all the interfaces of a Bay Router, it is possible to specify individual interfaces.

## Examples

Suppose a Wellfleet router well has three interfaces: E21, S21 and S22.



## Utilities

The user might wish to define (manually, in objects.C) two "virtual" routers, well1 and well2, as follows:

```
(well1
  :ipaddr well
  :if-1E21
)
(well2
  :ipaddr well
  :if-0S21
  :if-2S22
)
```

The list of interfaces to be loaded or unloaded is specified in the command line  
For example, the command:

```
fwell load p.W E21@well1
```

performs the following actions:

- unloads E21, S21, S22 (all the interfaces of the real router well — this is because the -u parameter was not specified)
- loads E21 (all the interfaces of the virtual router well1)

In practice, specifying E21 in the command line had no effect. All the interfaces were loaded, but as it happens, well1 has only one interface

**Note** - p.W is the name of the Rule Base file.

The command:

```
fwell load -u p.W well2
```

performs the following actions:

- unloads S21 and S22 (all well2 interfaces — this is because the -u parameter was specified)
- load S21 and S22 (all well2 interfaces)

The command:

```
fwell load -u p.W S21@well2
```

performs the following actions:

- unload S21 (the only interface specified in the command line)
- load S21 (the only interface specified in the command line)

### fw tab

fw tab displays the content of INSPECT tables on the target hosts in various formats.

Syntax

```
fw tab [-all | -conf confile] [-short] [-max num] [-u]
      [-table name] targets
```

Default format displays for each host: host name and a list of all tables with their elements

Explanation.

parameter	meaning
-all	Display all tables.
-conf confile	Read parameters from confile.
-short	Use short format: host name, table name, table ID, and its number of elements.
-max num	For each table, display only its first num number of elements (default is 16).
-u	Do not limit the number of displayed entries.
-table table_name	Display only table_name table.

Examples

```
fw tab
fw tab -t hostlist1 gateway1
```

### fwx1conf

fwx1conf is the FireWall-1 Address Translation configuration utility. For information about using fwx1conf, see "Configuring Address Translation — Command Line Interface" on page 189.

## Utilities

**snmp\_trap**

**snmp\_trap** sends an SNMP trap to the specified host. The message may appear in the command line, or as one line in the program input (stdin).

- **host** — the name of the host that should receive the trap
- **message** — the message sent to host.

```
Usage: snmp_trap [-v var] [-g generic_trap]
        [-s specific_trap] host [message]
```

**-v var**: an optional object id to bind with the message

**-g generic\_trap**: One of the values:

- 0 coldStart
- 1 warmStart
- 2 linkDown
- 3 linkUp
- 4 authenticationFailure
- 5 egpNeighborLoss
- 6 enterpriseSpecific (default value)

**-s specific\_trap**: a unique number specifying the trap type; valid only if generic trap value is enterpriseSpecific (default value is 0)

**snmp\_trap** is the default command in **SNMP Trap Alert Command** in the **Logging and Alerting** tab of the **Properties Setup** window (Windows GUI) and in the **Control Properties/Logging and Alerting** window (OpenLook GUI). You can use the **-v** flag to send the value of one of the FireWall-1 MIB variables (see "Firewall-1 MIB" on page 242).

**status\_alert**

**status\_alert** generates an alert. **status\_alert** is meant for use in the **Command** field of the **Status View Actions** window (see "Status View Actions" on page 149 of *Managing FireWall-1 Using the OpenLook GUI*) and in the **Action on Transition** field in the **Options** window (see "Options" on page 206 of *Managing FireWall-1 Using the Windows GUI*).

**fw converthosts**

`fw converthosts` converts a file in the `/etc/hosts` format to a file in the `dnsinfo.C` format. For information on why this might be needed as well as a description of the `dnsinfo.C` file format, see "DNS" on page 97 of *Virtual Private Networking with FireWall-1*.

## Syntax

```
fw converthosts < input_file > output_file
```

## Example

```
fw converthosts < /etc/hosts > /tmp/dnsinfo.C
```

**User Database - Importing and Exporting**

## Importing a User Database

To import users into the FireWall-1 User Database from an external source, you must create an ASCII (text) file with the required information and import the file into FireWall-1 using the `fw dbimport` utility.

The import file must conform to the following syntax:

- 1 The first line in the file is an attribute list.

The attribute list can be any partial set of the following attribute set, as long as name is included:

```
{name; groups; destinations; sources; auth_method; fromhour;
tohour; expiration_date; color; days; internal_password;
SKEY_seed; SKEY_passwd; SKEY_gateway; template; comments; userc}
```

- 2 The attributes must be separated by a delimiter character.  
The default delimiter is the `;` character. However, you can use a different character by specifying the `-d` option in the command line (see below).
- 3 The rest of the file contains lines specifying the values of the attributes per user.  
The values are separated by the same delimiter character used for the attribute list.  
An empty value for an attribute means use the default value.
- 4 For attributes that contain a list of values (for example, `days`), enclose the values in curly braces, that is, `{}`.

## Utilities

Values in a list must be separated by commas. If there is only one value in a list, the braces may be omitted.

A + or - character appended to a value list means add to delete the values in the list from the current default user values.

Otherwise the default action is to replace the existing values.

- 5 Legal values for the days attribute are: MON, TUE, WED, THU, FRI, SAT, SUN.
- 6 Legal values for the authentication method are: Undefined, S/Key, SecurID, Unix Password, FireWall-1 Password, RADIUS, Defender.
- 7 Time format is hh:mm.
- 8 Date format is dd-mm-yy, where mm is one of {Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec}.
- 9 If the S/Key authentication method is used, all the other attributes regarding this method must be provided.
- 10 If the FireWall-1 password authentication method is used, a valid FireWall-1 password should be given as well.  
The password should be encrypted with the G language encrypt function.
- 11 Values regarding authentication methods other than the one specified are ignored.
- 12 The userc field specifies the details of the user's SecuRemote connections, and has three parameters, as follows:

TABLE 10-4 userc parameters

parameter	values
key encryption method	FWZ1, DES, CLEAR, Any
data encryption method	FWZ1, DES, CLEAR, Any
integrity method	MD5,[blank] = no data integrity

"Any" means the best method available for the connection. This depends on the encryption methods available to both sides of the connection.

For example:

users	means
{FWZ1,FWZ1,MDS}	key encryption method is FWZ1; data encryption method is FWZ1; data integrity method is MD5
{DES,CLEAR,}	key encryption method is FWZ1; no data encryption; no data integrity
{Any,Any,}	use "best" key encryption method; use "best" data encryption method; no data integrity

**13** A line beginning with the ! character is considered a comment.

After preparing the import file, execute `fw dbimport` to import the users into the FireWall-1 User Database.

Syntax

```
fw dbimport [-m] [-s] [-v] [-r] [-k errors] [-f file] [-d delim]
```

Explanation

parameter	meaning
-m	Indicates that if an existing user is encountered in the import file, the user's default values will be replaced by the values in the template (the default template or the one given in the attribute list for that user in the import file), and the original values will be ignored. If -m is not specified, then an existing user's original values will be not be modified.
-s	Suppress the warning messages issued when an existing user's values are changed by values in the import file.
-v	verbose mode
-r	dbimport will delete all existing users in the database.
-k errors	Continue processing until nerror errors are encountered. The line count in the error messages starts from 1 including the attributes line and counting empty or commented out lines.
-f file	Specifies the name of the import file. The default import file is <code>\$FWDIR/conf/user_def_file</code> .
-d	Specifies a delimiter different from the default value (,).

To ensure that there is no dependency on the previous database values, use the -r flag together with the -m flag.



## Utilities

## Exporting a User Database

You can export your User Database to a file using `fw dbexport`.

The generated file can be in either of two syntaxes:

- the same syntax as the import file for `fw dbimport` (see "Importing a User Database" on page 285)
- LDIF syntax, which can be imported into an LDAP server



**Warning** – If you use the `-a` parameter (see below) to specify a list of attributes, and then import the created file using `fw dbimport`, the attributes not exported will be deleted from the user database.

## Exporting a User Database — dbimport syntax

## Syntax (dbimport syntax)

```
fw dbexport [ [-g group | -u user] [-d delim]
             [-a {attrib1, attrib2, ...} ] [-f file] ]
```

## Explanation (dbimport syntax)

parameter	meaning
<code>-g</code>	Specifies a group of users to be exported; users are not exported.
<code>-u</code>	Specifies that only one user (user) be exported.
<code>-d</code>	Specifies a delimiter different from the default value (",").
<code>-a</code>	Specifies the attributes to export, in the form of a comma-separated list between {} characters, for example, <code>-a {name, days}</code> . If there is only one attribute, the {} may be omitted.
<code>-f</code>	Specifies the name of the output file. The default output file is <code>\$FWDIR/conf/user_def_file</code> .

## Exporting a User Database — LDIF syntax

## Syntax (LDIF syntax)

```
fw dbexport -l [ [-g group | -u user] [-d delim]
                 [-a {attrib1, attrib2, ...} ] -s subtree [-f file]
```

## Explanation (LDIF syntax)

parameter	meaning
-l	Create an LDIF format file for importation by an LDAP server.
-g	Specifies a group of users to be exported; users are not exported.
-u	Specifies that only one user (user) be exported.
-A [-i]	Specifies that all users are to be exported. -i specifies that all groups are to be exported as well.
-s	Specifies the branch under which the users are to be added.
-a	Specifies the attributes to export, in the form of a comma-separated list between {} characters, for example, -a {name, days}. If there is only one attribute, the {} may be omitted.
-f	Specifies the name of the output file. The default output file is \$FWDIR/conf/user_def_file.

## Example (LDIF syntax)

```
fw dbexport -l -u maryj -s o=WidgetCorp,c=us
```

creates a file consisting of one entry, where the DN is:

```
cn=maryj,o=WidgetCorp,c=us
```

## Notes

The LDIF file is a text file which you may wish to edit before importing it into an LDAP server. For example, in the FireWall-1 user database, user names may be what are in effect login names (such as "maryj") while in the LDAP server, the DN should be the user's full name ("Mary Jones") and "maryj" the login name.

Another issue is that you may wish to import different groups of users into different branches. In this case, you should run fw dbexport more than once, for example:

```
fw dbexport -f f1 -l -g marketing -s ou=marketing,
o=WidgetCorp,c=us
fw dbexport -f f2 -l -g rnd -s ou=rnd,o=WidgetCorp,c=uk
```

Next, import the individual files into the LDAP server one after the other. For information on how to do this, refer to the documentation for your LDAP Server.

Utilities

290 FireWall-1 Architecture and Administration • September 1998

CHAPTER **11**

# INSPECT

## In This Chapter

<i>Introduction</i>	<i>page 291</i>
<i>INSPECT Reference Manual</i>	<i>page 298</i>

## Introduction

A FireWall-1 Security Policy is defined by a Rule Base and the properties of the objects (networks, services, hosts, and users) used in the Rule Base. Typically, the system administrator defines a Security Policy using the FireWall-1 GUI (Graphical User Interface). From the Security Policy, FireWall-1 generates an Inspection Script written in the FireWall-1 Language (INSPECT). Inspection Scripts are ASCII files and can also be written using a text editor.

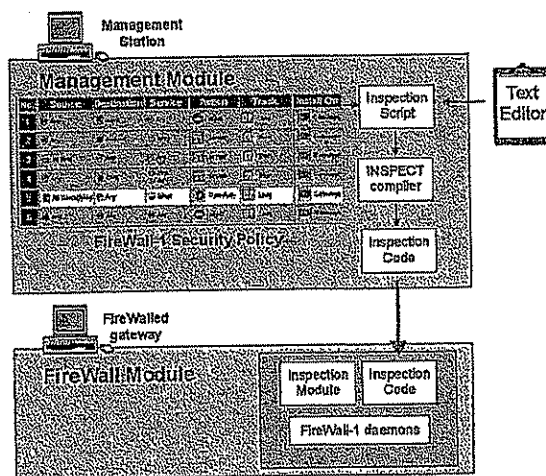
Inspection Code, compiled from the Inspection Script, is then transmitted on a secured control channel from the FireWall-1 Management Center — the computer on which the Security Policy was defined — to the FireWall-1 daemons on the network objects that will enforce the policy. The FireWall-1 daemon loads the Inspection Code into the FireWall-1 FireWall Module.

INSPECT was designed specifically as a firewall language, and so it enables typical firewall actions (for example, accept, reject, log, *etc.*). To meet reliability and efficiency requirements, INSPECT has the following characteristics:

- There are no loops.
- Functions do not support recursion.
- Only a limited form of indirect access is allowed.
- Conditions are short circuits.
- There is no explicit memory allocation.
- Function argument passing is by value only.
- A function returns exactly one value.

## Introduction

- Source code is in a single file (except that the C-preprocessor #include directive is allowed), and there is no external linkage.
- The name space (that is, macros, functions, tables and formats) begins at the end of its definition and persists to the end of the file.



**FIGURE 11-1** FireWall Inspection Components - flow of information

The ability to directly edit Inspection Scripts facilitates debugging and enables administrators to tailor Inspection Scripts to their specialized requirements. The rest of this chapter describes the INSPECT language.

**TABLE 11-1** FireWall Inspection Components

Component	Description
Inspection Script	ASCII file (*.pf) in the INSPECT language which is either generated from a Security Policy (*.w file), hand written or some combination of the two
Inspection Code	a file (*.fc) compiled from an Inspection Script (*.pf)
FireWall Module	a FireWall-1 software module running on a FireWalled host that executes Inspection Code

## Writing an Inspection Script

The only way to learn a new language is by writing programs in the language. INSPECT is a firewall language, so testing your program requires that you create the program text, successfully compile it, load it to a FireWalled host and verify that the Inspection Code does what you expect it to do. Once you have mastered the details of these mechanical steps, everything else is relatively straightforward and simple.

## Writing an Inspection Script

## A Simple Script

An Inspection Script corresponds to a Security Policy, and its most important elements are rule statements. The following script consists of a single rule statement:

```
accept [ 9 : 1 ] = 6;
```

This rule statement is read as "accept the packet if the value at byte 9 (for a length of 1 byte) is equal to 6." (In IP packets, byte 9 identifies the protocol, and a value of 6 indicates a TCP packet.) In short, the script accepts TCP packets.

## Testing the Script

To test this simple INSPECT script, proceed as follows:

- 1 Use the `fwc` command to compile the Inspection Script (`fwc name.pf`).

The `fwc` command puts the Inspection code in `$FWDIR/tmp`. Your simple INSPECT script should compile successfully with no errors.

**Note** – For additional information about the `fwc`, `fwstart` and `fw load` commands, see Chapter 10, "Command Line Interface."

- 2 Verify that your host is FireWalled.

Use the `fwstart` command to start the FireWall module.

- 3 Use the `fw load` command to compile the Inspection Script and install the resulting Inspection Code in a single step (`fw load name.pf`).

- 4 Verify that only TCP packets are allowed to access the current host.

For example, the TELNET protocol is accepted and the PING protocol is rejected.

## INSPECT Syntax

INSPECT's syntax is similar to that of C, but there are differences between the two languages. The rule statement shown above illustrates some of them:

- the `=` operator means test for equality (rather than assignment)
- the test `{ [ 9 : 1 ] = 6 }` is *not* preceded by the `if` keyword

Since INSPECT uses the C preprocessor (see "Preprocessor" on page 316), the script shown above might be rewritten as follows:

```
#define tcp ({ 9 : 1 ] = 6 )
accept tcp;
```



## Introduction

In this script, a pre-processor macro named `tcp` is defined (using the pre-process `#define` directive), and then used in the `accept` statement. This version of the rule statement is simpler and more readable than the first version.

Taking the idea of using macros one step further, the script might again be rewritten, as follows:

```
#define ip_p [ 9 : 1]
define tcp { ip_p = 6 };
accept tcp;
```

In this version, a macro (`ip_p`) representing the byte that specifies the protocol is defined, and then `tcp` is defined in terms of `ip_p`.

**Note** - `#define` is a C preprocessor directive and `define` is an INSPECT statement. The difference between them is discussed under "define" on page 311.

This two stage definition is useful because it simplifies defining additional protocols, as follows:

```
define tcp { ip_p = 6 };
define udp { ip_p = 17 };
define icmp { ip_p = 1 };
```

## Compound Conditions

A rule statement's condition may be more complicated. For example,

```
accept (tcp, telnet);
```

means: accept the packet if it is both TCP and TELNET. The comma (,) is the logical AND operator.

**Note** - `telnet` and `ftp` are defined in the file `base.def`.

Here is another example:

```
accept (tcp, telnet or ftp);
```

This statement means: accept the packet if it is TCP and either TELNET or FTP.

## Writing an Inspection Script

This statement illustrates the only difference between operator precedence in C and INSPECT. In C, the expression:

```
X && Y || Z // read as "X AND Y OR Z"
```

is understood as ((X AND Y) OR Z), that is, AND takes precedence over (is evaluated before) OR.

In INSPECT, the expression:

```
X and Y or Z
```

is understood as (X AND ((Y OR Z))), that is, OR takes precedence over AND.

Parentheses — "(" and ")" — can be used to force operator precedence. There is no penalty for superfluous parentheses.

Here is a rule statement that illustrates the use of parentheses to force operator precedence:

```
accept (tcp, telnet or ftp) or (udp, snmp);
```

This statement would have quite a different meaning without the parentheses.

The next rule statement looks almost like a rule in the Rule Base Editor:

```
accept                                     // Action
(tcp, telnet or ftp),                     // Services
((ip_src = doors) or (ip_src = well)),    // Source
(ip_dst = natasha);                       // Destination
```

The first four elements of a rule in the Rule Base (Action, Source, Destination and Services) are expressed in the above rule statement.

**Note** — The definitions of `ip_src` and `ip_dst` are not shown here. INSPECT comments have the same syntax as C++ comments.

#### Elements of a Rule

In the Rule Base Editor, a rule is composed of six elements, as follows:

**Source** — where the packet is coming from

**Destination** — where the packet is going

## Introduction

**Services** — the type of application

**Action** — what is to be done with the packet

**Track** — whether to log the packet or generate an alert

**Install On** — the FireWall Module or Inspection Module that will enforce this rule

You have already seen how the first four elements are expressed in an INSPECT rule statement.

From the point of view of INSPECT's syntax, none of the elements in a rule statement is required. Even a rule statement without an Action can "do something" as a side effect of a condition.

## Track

A rule's Track element is often set to one of the log options. Though there is a log operator in INSPECT, it's more convenient to use the LOG macro, as follows:

```
#include "fwui_head.def"
SRV_tcp(telnet, 23)
SRV_tcp(ftp, 21)
accept                                     // Action
(tcp, telnet or ftp),                      // Services
(ip_src = doors or ip_src = well),        // Source
(ip_dst = natasha),                       // Destination
LOG(long, LOG_NOALERT, 1);                // Track
```

The SRV\_tcp(telnet, 23) statement defines telnet, and SRV\_tcp(ftp, 21) defines ftp.

For a description of the LOG macro, see "LOG" on page 316.

The #include statement in the script shown above includes the standard macro definitions. The script is complete and will compile without errors, if the names doors, well, and natasha can all be resolved. (For more information about #include, see "#include" on page 317).

## Scope (Install On)

The last element in a rule is Install On, the FireWalled objects that will enforce the rule. This element is known as the rule's scope, and its syntax is:

```
direction interfaces@hosts
```

## Writing an Inspection Script

TABLE 11-2 Scope Elements

element	meaning
direction	inbound (or =>) — incoming outbound (or <=) — outgoing eitherbound (or <>) — incoming and outgoing
interfaces	on which network interface(s) to examine packets
@	required separator
hosts	on which host(s) to examine packets

The scope is specified before the action, as follows:

```
#include "fwui_head.def"
SRV_tcp(telnet, 23)
SRV_tcp(ftp, 21)
inbound all@natasha           // Install On (scope)
accept                        // Action
  (tcp, telnet or ftp),       // Services
  (ip_src = doors or ip_src = well), // Source
  (ip_dst = natasha),         // Destination
  LOG(long, LOG_NOALERT, 1);   // Track
```

The scope shown above specifies the rule's scope as inbound packets on all interfaces of the FireWalled host natasha.

inbound, outbound and eitherbound are all macros defined in fwui\_head.def.

# **EXHIBIT 3**

## **PART 5**

## INSPECT Reference Manual

## include Files

The \$FWDIR/lib directory contains a number of files that are always included by Inspection Scripts generated by FireWall-1. You may find it useful to include some of these files in Inspection Scripts you write yourself.

TABLE 11-3 Some Useful include Files

file name	meaning
fwui_head.def	contains many useful macro definitions — also includes other *.def files
formats.def	contains definitions of log formats that are used in FireWall-1 User Interface, for example, the definitions of the Long format and the Short format
code.def base.def	contain the core logic of the Inspection Module
fwui_trail.def	contains the implicit drop rule — usually included at the end of an Inspection Script

## INSPECT Reference Manual

## Introduction

An INSPECT script is compiled into low level code which is run on a stack-based virtual machine.

The virtual machine is placed in the FireWalled machine's kernel. The virtual machine inspects every IP packet passing through the machine by running the code compiled from the Security Policy.

Since FireWall-1 runs on machines with a 32-bit word length, each stack cell is 32-bits wide. INSPECT uses the stack for storing intermediate values. Other storage areas used by INSPECT are registers and tables (as described later).

INSPECT supports 32-bit integers, as well as other special constants (for example, IP-addresses, interfaces, etc.).

## Lexical Conventions

The INSPECT compiler is a single phase compiler. A program consists of a single source file (except for C pre-processor #include file) and is translated in two stages. The first stage is a preprocessor stage, during which the C-preprocessor directives are carried out. In the second stage, the INSPECT Script is transformed into Inspection Code.

INSPECT comments have the same syntax as C++ comments. The characters // introduce a comment.



**Reserved Words**

The following words (all in lower case only) are reserved words in INSPECT:

**TABLE 11-4** INSPECT Reserved Words

accept	and	call	date
day	deffunc	define	delete
direction	domains	drop	dynamic
expcall	expires	export	format
from	fwline	fwrule	get
hold	host	hosts	if
ifaddr	ifid	in	interface
interfaces	keep	limit	log
modify	netof	nets	nexpires
not	or	packet	packetid
pass	record	refresh	reject
set	static	to	tod
vanish	xor		

In addition, the following are also reserved words:

- names of the days of the week (for example, Sunday, sunday and sun),
- names of the months
- constructs of the form [S|s][r|R]n (where n is a decimal number)

It is recommended that you use service and protocol names for their original purpose, that is, when using telnet, ftp, etc, do not hide the system constants (for example, avoid using these names for network objects).

**Constants****Numeric Constants**

There are no floating point constants in INSPECT.

Integer constants can be expressed in the standard formats:

- A number beginning with 0x is understood as a hexadecimal integer, for example 0x4f.
- A number beginning with 0 is understood as an octal integer, for example 0777.
- Otherwise, numbers are understood as decimal integers.

**Time Specification**

Three decimal integers separated by two colons (for example, 23:30:00) are understood as a time constant.

## INSPECT Reference Manual

**Day in Month Specification**

Three character abbreviations or full month names, followed by a day number (for example, Jan 22) are understood as a time constant.

**Day in week Specification**

Three character abbreviations or full day names (for example, sun) are understood as a time constant.

**Special FireWall constants**

Since INSPECT is designed especially for FireWall purposes, it recognizes the following special communication entities.

- domains
- nets and hosts (expressed as IP-address constants)
- interfaces

Network and communication entities may be used as special constants in either lists or expressions. Special purpose commands that handle some of these entities are described later.

**IP address constant**

Four decimal integers separated by three periods (for example, 192.0.0.24), or three decimal integers separated by two periods (for example 192.0.0), or two decimal integers separated by one period (for example, 192.0) are considered constants and are understood as IP addresses.

**Identifiers****Types**

There are five types of identifiers in INSPECT:

- segment registers
- special purpose registers
- dynamic and static tables
- macros
- functions

**Meaning of Identifiers**

Identifiers or names refer to variety entities: functions, macros, tables, registers, *etc.* In contrast to function and macro identifiers, tables and registers are storage area designed for the programmer. The compiler is responsible for handling (that is, allocating) these storage areas and the programmer may only store, remove and retrieve data.

## Writing an Inspection Script

Indirect access is limited to storing relative addresses in segment registers (see "Segment Registers" on page 301). The value of a segment register may be interpreted as a relative address in a packet or as a table number (the `set` command may be used to store these values in a segment register). Some of the INSPECT expressions use segment registers for indirect access.

For example,

```
sr6.[12:1]
```

refers to byte (12 + the contents of segment register `sr6`).

## Names

Identifier names are case-sensitive. INSPECT does not impose a limit to a name's length.

## Name Resolution

The compiler tries to resolve names using various external databases, such as `/etc/services`, based on the context in which the name is used. If a name is defined as an INSPECT identifier (for example, a table, macro, or function) then this definition hides the database value of the name.

## Segment Registers

A segment register is defined as follows:

```
segment-register:
s[r|R]n
```

where `n` is a decimal number between 0 and 15. For example, `sr6` and `sr13` are valid segment register names, but `sr16` is not.

Unlike other INSPECT identifiers, segment register names are not case sensitive. So, `Sr3`, `sr3` and `sr3` all refer to the same segment register.

A segment register is used to store a base value from which offsets in an expression are calculated. For example, the expression:

```
{12:2}
```

## INSPECT Reference Manual

refers to 2 bytes beginning at byte 12 of the packet (the first byte is at byte zero), while:

```
sr6.[12:2]
```

refers to 2 bytes beginning at byte (12 + the contents of segment register sr6).

A segment register can be used to store a value for later use. For example:

```
set sr1 [12];
accept sr1 = [14,1];
```

This means: accept the packet if byte 12 equals byte 14.

## Functions

INSPECT uses functions for two primary reasons:

- to break large computing tasks into smaller ones, clarifying the code
- to decrease the size of the Inspect code

The INSPECT deffunc operator is evaluated similarly to define but outputs a code rather than identifying inline code.

Consider the following script:

```
#define ip_p [ 9 : 1]
deffunc tcp {ip_p = 6};
accept tcp;
```

The generated code contains a function that checks if the current packet is a TCP packet.

In INSPECT, every function returns exactly one value. The Inspection Code starts by calling the function tcp and then applies the accept statement on the value returned from the function.

Function parameter passing is strictly by value; so, for example, formats cannot be passed as arguments to a function. No recursion is allowed. Moreover, functions must be defined before they are called and there are no function prototypes.

## Tables

There are two types of tables: dynamic (see "Dynamic Tables" on page 304) and static (see "Static Tables" on page 307).

A table consists of attributes and entries.

## Writing an Inspection Script

## Attributes

TABLE 11-5 lists the possible attributes of a FireWall-1 table.

TABLE 11-5 FireWall-1 Table Attributes

attribute name	meaning
expires	An entry is removed from the table if it is not accessed in this period of time.
refresh	reset the expiration timeout when accessed
free function <i>x</i>	Call this function when an entry is deleted or expires.
hashsize	size of the hash — should be close to table size.
modtrap <i>x</i>	Trap the FireWall-1 daemon when the table is modified.
intrap <i>x</i>	Trap the FireWall-1 daemon when adding an entry.
outtrap <i>x</i>	Trap the FireWall-1 daemon when deleting an entry.
keep	Keep the table's entries after a Security Policy is installed.
kbuf <i>x</i>	The <i>x</i> <sup>th</sup> argument in the value section is a pointer to an internal data structure (primarily used in encryption).
implies <i>table_name</i>	A entry deleted from this table will be deleted from <i>table_name</i> table as well.
limit <i>x</i>	Limit this table to <i>x</i> entries.
synch	Synchronize this table if using FireWall-1 synchronization.

## Entries

An entry can be in the form of a tuple, or of a tuple and a value. Tables are associative — that is, an entry is identified by its value rather than by its position in the table.

For example,

<12,24,36>

is a tuple with 3 elements, while:

<12,24;36>

is a tuple with 3 elements, of which the last (36) is the value.

A value may itself be a tuple, for example <12,24;36,48>.

## INSPECT Reference Manual

The action:

```
record <12,24,36> in udp_tab;
```

puts the 3 element tuple <12,24,36> in the table udp\_tab (where 36 is the value and <12,24> is the key).

The expression:

```
udp_tab [12,24]
```

returns the table value (in this case the singleton <36>) whose key is <12,24>.

When the value is a tuple, the get statement is used. The expression:

```
get <12,24,36> from udp_tab to sr1
```

returns each of the values from the <12,24,36> entry in udp\_tab into the segment registers starting with sr1, sr2 and so on. For example, if the value is a tuple with three elements, the first is stored in sr1, the second in sr2 and the third in sr3.

A table must be explicitly defined before it is used (see examples below). Only dynamic tables support values.

INSPECT has special operators for testing the content of tables and for extracting table values. The expression:

```
udp_tab [12,24]
```

returns the table value whose key is <12,24> and the expression:

```
<12,24> in udp_tab
```

tests if the table contains an entry whose key is <12,24>.

A table must be explicitly defined before it is used.

### Dynamic Tables

A dynamic table is one whose entries change as the Inspection Code is being executed. The number of entries (or tuples) in a dynamic table is not fixed when the table is created, and tuples can be freely added and deleted.



## Writing an Inspection Script

To create a dynamic table, define one using the dynamic keyword. For example, the expression:

```
ThisTab = dynamic {};
```

creates a dynamic table named ThisTab. The table's tuples are not specified when the table is defined because tuples are added and deleted dynamically.

An optional list of attributes may be specified after the {}. The attributes are:

`expires n` — tuples not updated or written for `n` seconds are deleted

If this attribute is specified for a table, it can be overridden for individual elements (see "Adding an Element to a Dynamic Table" on page 306).

`refresh` — reset the expiration timer on each use (read or write)

`limit` — sets the maximum number of elements the table can contain

`nexpires` — elements do not expire, but are removed only when explicitly deleted

`nexpires` is the default setting.

`keep` — do not reset this table when the Security Policy is re-installed

When a Security Policy is installed on a FireWalled host on which a Security Policy is already installed, the tables are all reset. A table will not be reset if both of the following conditions are true:

- the table was defined with the `keep` attribute
- the table's name and sequential number (internally assigned by FireWall-1 to each table in accordance with its position in the Inspection Script) are unchanged

`expcall` — call the given (by number) kernel functions when a table element expires (see "call" on page 311)

## Defining a Dynamic Table

For example, to define a dynamic table whose tuples expire if they are not used for 60 seconds:

```
udp_out = dynamic {} expires 60 refresh;
```

## Table Operations

INSPECT has special commands for modifying the contents of a table.

## INSPECT Reference Manual

## Adding an Element to a Dynamic Table

To record a tuple in the dynamic table:

```
record <src,sport,dst> in udp_out;
```

To record a tuple in the dynamic table with an expiration timer different from the default expiration timer for the table:

```
record <src,sport,dst @timeout> in udp_out;
```

where timeout is the number of seconds.

To modify a tuple in the dynamic table without resetting the expiration timer to zero:

```
record <12,24;36> in udp_tab;
```

## Checking if an Element is in a Dynamic Table

To check if a tuple is in a dynamic table:

```
<src,sport,dst> in udp_out;
```

## Deleting an Element from a Dynamic Table

To delete a tuple from the table:

```
delete <src,sport,dst> from udp_out;
```

## Example

Here is a simple but powerful example of the use of dynamic tables.

```
#include "fwui_head.def"
udp_out = dynamic {} expires 60 refresh;
accept udp,direction = 1,record <src,sport,dst> in udp_out;
accept udp, direction = 0,<dst,dport,src> in udp_out;
```

- The context tuple (source, port, and destination) of every outgoing UDP packet (direction = 1) is recorded in the dynamic table udp\_out.

## Writing an Inspection Script

- A context tuple is deleted after 60 seconds if no corresponding UDP packet is encountered.
- An incoming UDP packet (`direction = 0`) is accepted only if its context tuple is in `udp_out` (in other words, if it is a reply to a previously registered outgoing packet).

**Note** – INSPECT short-circuits compound AND conditions as soon as it encounters a FALSE condition, so the record will only execute if `direction = 1` is TRUE. The order of the expressions is important here.

For an explanation of `direction`, see “Current Packet” on page 310.

## Static Tables

A static table is one whose elements are fixed when the table is created, and cannot be added and deleted.

To create a static table, define one using the `static` keyword. A comma-separated list of constant expressions must be specified between the brackets.

For example:

```
GWList = static{gatekeeper, gatekeeper_le0, gatekeeper_le1 };
```

## Lists

A list is a typed static table. The available types are:

- domains
- nets
- hosts
- interfaces
- format

For example:

```
domain_list = domains { .security.com, .iconnet.com };
```

is a domain list. Having defined the list, the condition:

```
ip_src in domain_list
```

tests whether `ip_src` (the packet's source IP address) belongs to the domain defined by the given networks (`.security.com` and `.iconnet.com`).

## INSPECT Reference Manual

Similarly, for a "proper" network (that is, a network whose netmask is the one implied by its class), you can write:

```
net_list = nets { 192.9.200.0, 10.0.0.0, 132.64.0.0 };
```

Then the statement

```
ip_dst in net_list
```

tests whether `ip_dst` belongs to one of the networks in `net_list`.

## Format Lists

A format list is a list used in creating log records.

For example, the format list (defined in `$FWDIR/lib/formats.def`):

```
short = format {
  <"proto", proto, ip_p>,
  <"src", ipaddr, src>,
  <"dst", ipaddr, dst>,
  <"service", port, dport>
};
```

defines a format named `short`, which consists of a list of four tuples. Each format list tuple is made up of three elements., as follows:

label (for example "src")

type (from a list of predefined types):

- `int` — decimal 32 bit signed integer
- `uint` — decimal 32 bit unsigned integer
- `hex` — hexadecimal representation of a 32 bit unsigned integer
- `ipaddr` — an IP address
- `service, port` — tcp or udp port number
- `proto` — IP protocol number
- `string` — an ASCII string (not used in the FireWall Module)

The first two elements of each tuple are used in creating a log dictionary — a record which describes log records. The last element is the actual value written to the log.

The pre-defined format lists are in the file `$FWDIR/lib/formats.def`.

See also "LOG" on page 316 and "log" on page 313.

## Operators

The following operators are available in INSPECT:

TABLE 11-6 FireWall-1 Language Operators

operator	Meaning	operator	Meaning
+	addition	>>	shift right
-	subtraction	<<	shift left
/	division		
*	multiplication	()	function call
%	modular division	[]	table indexing (for example, <code>udp_tab[12,24]</code> )
&	bitwise AND	<> and ><	in-out
	bitwise OR	= and is	equal
^	bitwise XOR	!= and is not	not equal
.	logical AND	=>	incoming
<	less than	or	logical OR
>	greater than	xor	logical XOR
<=	outgoing or less than or equal to (depending on context)		
>=	greater than or equal to		

## Date and Time

Certain operators return information about the current date and time, as follows:

- `date`— day of the month (0 – 30, where 0 is the first day of the month)
- `day`— day of the week (0 – 6, where 0 is Sunday)
- `tod`— time of day (for example, in the statement `tod < 08:00:00`)

## INSPECT Reference Manual

## 'Current Packet'

Rule statements operate on the current packet, that is, the packet being inspected. Certain operators return information about the current packet, as follows:

- direction — 0 (inbound) or 1 (outbound)
- host — canonical IP address of the machine on which the FireWall Module is running
- ifaddr — packet's interface address
- interface — packet's interface (le0, le1, etc.)
- packetid — a unique number assigned to a packet by FireWall-1 as the packet passes through an interface

## INSPECT Commands

INSPECT enables you to define functions in an INSPECT script. The differences between functions and macros are:

- Macros are faster than functions, since there is no pushing and popping of parameters on the stack.
- Using macros gives Inspection Scripts a simple linear structure.
- Using macros avoids recursion problems.
- Using functions leads to smaller Inspection Scripts.

For information on defining macros, see "define" on page 311.

For information on defining functions, see "deffunc" on page 311.

## accept

The accept action accepts a packet. For example:

```
accept (tcp, telnet or ftp);
```

accepts the packet if the condition (tcp, telnet or ftp) is TRUE. See also the descriptions of the vanish and drop actions in this section.

A more complex use of accept is this:

```
accept ((condition-list)
or      (TRAP(parameter-list),drop));
```

If the conditions in condition-list are all TRUE, then the packet is accepted, otherwise the TRAP macro is executed and the packet is dropped. This technique (putting the drop statement in the accept statement) is used when the TRAP macro

## Writing an Inspection Script

can be expected to modify a table in such a way that when the dropped packet is re-transmitted, the conditions in condition-list will all be TRUE and the packet will be accepted.

## call

The call command enables an Inspection Script to call an externally defined function, identified by the first argument. The call command is used extensively to support encryption.

The syntax of the call command is:

```
call (<function number>; <tuple of arguments>)
```

## deffunc

An INSPECT function is defined in exactly the same way an INSPECT macro (as opposed to a preprocessor macro) is defined, except that deffunc is used instead of define. The difference is that define is expanded inline and deffunc is expanded out of line.

## Compatibility

FireWall-1 supports the deffunc statement starting with Version 2.1, but earlier versions do not. This means that:

- Inspection Scripts generated by FireWall-1 Version 2.1 and higher will not compile under earlier versions.

To compile your Version 2.1 and higher Inspection Scripts (under Version 2.1 and higher) so that the compiled code will run under earlier versions, add the following pre-processor directive in \$FWDIR/lib/fwui\_head.def:

```
#define deffunc define
```

This directive changes all the function definitions in the script to macro definitions.

- Inspection Code compiled from Inspection Scripts generated by Version 2.1 and higher will not run under earlier versions.

## define

The pre-processor #define directive removes the #defined entity from the compiler's input before compilation. In contrast, the INSPECT define operator is evaluated during compilation and assigns a meaning to an entity in a particular context.



## INSPECT Reference Manual

Consider the following script:

```
#include "fwui_head.def"
#define ip_p [ 9 : 1]
define tcp {ip_p = tcp};
accept tcp;
```

The use of the token `tcp` twice in the `define` statement is unambiguous because:

- The compiler knows the meaning of `tcp` from its internal tables.
- The compiler resolves `{ip_p = tcp}` first.

The compiler understands the `accept` statement because the only meaning of `tcp` known to the compiler when it encounters the statement is appropriate to the context in which `tcp` is used.

Consider the following script:

```
#include "fwui_head.def"
#define ip_p [ 9 : 1]
define tcp {ip_p = 6};
accept (ip_p = tcp);
```

Though `tcp` has two possible meanings in this script, the `accept` statement still compiles correctly because only one meaning is appropriate to the context.

`drop`

The `drop` action drops a packet without notifying the sender. For example:

```
drop (net_in(ip_src, cp_net_128, cp_net_128_netmask))
```

drops the packet if the condition `(net_in(ip_src, cp_net_128, cp_net_128_netmask))` is TRUE. See also the descriptions of the `vanish` and `accept` actions in this section.

`export`

The statement:

```
export { } .xxx ;
```

copies everything in the block — between the `{` and the `}` — to the file `<name>.xxx`, where `name` is the name of the file being compiled (without the `.pf` suffix).

## Writing an Inspection Script

For example, the statement:

```
export {} .set
```

in the file `abcdef.pf` copies the block to `abcdef.set`.

`export` is used to make data that is not part of the Inspection Code available to the FireWall Module. The `export` statement usually appears at the beginning of Inspection Scripts generated by FireWall-1.

`hold`

The `hold` action holds a packet in the kernel. The packet is neither passed nor rejected. Its status can only be changed by the FireWall-1 daemon.

`in`

The `in` operator tests whether a value is in a table. For example, the statement:

```
<dst,dport,src> in udp_out;
```

tests whether the tuple is in the `udp_out` table.

`log`

The `log` command creates a log record in the specified format. For example,

```
log short;
```

creates a log record in the `short` format. The values of the expressions in the third elements of the format tuples are written to the log record. In addition, the following standard fields are also written to the log record:

- timestamp
- address of FireWalled host (or gateway) that created this log record
- interface
- direction
- action

The first two elements in each format tuple are used in creating a log dictionary, that is, a record which describes log records. A single log file may contain many dictionaries, each of which describes a different set of log records in the file.

See also "Format Lists" on page 308 and "LOG" on page 316.

## INSPECT Reference Manual

## modify

The `modify` command adds a tuple to a dynamic table (as the `record` operator does). If the tuple already exists, the expiration timer is not reset to zero (in contrast to the `record` operator). This is true even if the table is defined with the `refresh` attribute.

For example:

```
modify <src,sport,dst> in udp_out;
```

## netof

The `netof` operator tests whether an IP address is a part of a network. For example, the statement:

```
(netof ip_src = big-net)
```

tests whether `ip_src` is part of the network `big-net`, according to the network mask implied by `big-net`'s class.

## set

The `set` command assigns a value to a segment register. For example:

```
set sr6 12;
```

assigns the value 12 to the segment register `sr6`.

## record

The `record` command adds a tuple to a dynamic table. If the tuple already exists, the expiration timer is reset to zero (in contrast to the `modify` operator). For example:

```
record <src,sport,dst> in udp_out;
```

adds the tuple `<src,sport,dst>` to the dynamic table `udp_out`.

## reject

The `reject` action rejects a packet. For example:

```
reject(top, ident);
```

## Writing an Inspection Script

If the condition (tcp, ident) is TRUE, then reject drops the packet and for TCP, signals the originator that the attempt was forcibly denied.

vanish

The vanish action drops a packet without a trace, and for packets of an established TCP connection, does not perform the mangling described in Chapter 12, "Miscellaneous Security Issues." The drop and reject actions do perform this mangling for packets of an established TCP connection.

### Big Endian and Little Endian

"Big Endian" and "Little Endian" are terms which describe two different hardware conventions for storing data.

#### Big Endian

Given the following data at these memory addresses:

data	1	2	3	4
address	1000	1001	1002	1003

In the Big Endian convention, the data types at memory address 1000 have these values:

long integer	1234
short integer	12
byte	1

#### Little Endian

Given the same data, in the Little Endian convention, the data types at memory address 1000 have these values:

long integer	4321
short integer	21
byte	1

When Used

In the expression:

[12, b]

the b indicates that the word (4 bytes, the default length when no length is specified) is to be treated as a Big Endian integer.

## INSPECT Reference Manual

To ensure portability, always use `b` when referring to data in the header of any Big Endian protocol, for example, TCP/IP.

**Macros****LOG**

The `LOG` macro (defined in the file `fwui_head.def`) takes three arguments:

- `format` — the type of log: long or short
- `alert` — the type of alert to issue

The value `LOG_NOALERT` is predefined.

- `rule number` — the number of the rule in the Rule Base invoking the tracking

The `LOG` macro has the following advantages over the `log` operator:

- The `LOG` macro automatically handles the rule number.
- The `format` takes into account the type of packet and writes the appropriate information (program number for RPC, type and sub-type for ICMP and port number for others) to the log.
- `LOG` takes into account the **Excessive Log Grace Period** parameter in the **Control Properties/ Logging and Alerting** window.

See also "Format Lists" on page 308 and "LOG" on page 316.

**TRAP**

`TRAP` calls a routine in the FireWall-1 daemon which typically loads a value into a table.

**Preprocessor****Pre-processor statements**

INSPECT uses the C preprocessor to preprocess the Inspection Script source file before compiling it. The following C pre-processor directives have no meaning in the context of a FireWall-1 Inspection Script:

```
#error
#line
#pragma
```

The pre-processor directives most commonly used in a INSPECT script are given below:

## Compiling and Installing

#define

#define XYZ(a,b,c) expression // with parameters

or

#define XYZ expression // without parameters

#include

#include "fwui\_trail.def"

## Conditional Compilation

You can use the pre-processor #ifdef directive to conditionally compile parts of an Inspection Script. The following symbolic constants are defined in each environment:

**Compiling and Installing**

To compile an Inspection Script (\*.pf file), use the fwc command, which compiles an Inspection Script but does *not* install the resulting Inspection Code (\*.fc file).

To compile an Inspection Script and install the resulting Inspection Code in a single step, use the fw load command.

For additional information about these commands, see Chapter 10, "Command Line Interface."

INSPECT Reference Manual

318 FireWall-1 Architecture and Administration • September 1998



**CHAPTER 12**

# Miscellaneous Security Issues

---

**In This Chapter**

<i>Default Security Policy</i>	<i>page 319</i>
<i>Auxiliary Connections</i>	<i>page 321</i>
<i>Established TCP Connections</i>	<i>page 322</i>
<i>The Fast Mode Option</i>	<i>page 325</i>
<i>Generic User</i>	<i>page 325</i>
<i>Redirecting Logging to Another Master</i>	<i>page 327</i>
<i>The TCP SYN Flooding Attack</i>	<i>page 329</i>

**Default Security Policy****The Period of Vulnerability**

During the boot process, there is a short period of time (measured in seconds) between the point when the gateway becomes able to communicate and the point when the FireWall-1 Security Policy is loaded and is enforced. During this time, (the period of vulnerability) both the gateway and networks behind the gateway are vulnerable to attack, unless you take measures to protect them.

**Protecting the Network**

You can protect networks behind the gateway by disabling IP Forwarding in the OS kernel and allowing FireWall-1 to control IP Forwarding. If you do this, there will never be a time when IP Forwarding is on but your Security Policy is not being enforced, so networks behind the gateway are safe.

## Default Security Policy

### Protecting the Gateway

Disabling IP Forwarding protects networks behind the gateway, but it does not protect the gateway itself. For this purpose, FireWall enables you to implement a minimal default Security Policy during the period of vulnerability.

### Standard Default Security Policies

When you install the FireWall Module, you are asked to choose between two default Security Policies:

#### 1 drop

The drop default Security Policy drops all communications in and out of the gateway during the period of vulnerability.

If the boot process requires that the gateway communicate with other hosts, then the drop default Security Policy should not be used.

#### 2 accept

The accept default Security Policy allows:

- all outgoing communications
- incoming communications on ports through which there were previous outgoing communications
- ICMP packets
- broadcast packets

### User Defined Default Security Policies

You can define your own default Security Policy as follows:

#### 1 Create an INSPECT script named defaultfilter.pf in \$FWDIR/conf.

The script may not perform any of the following functions:

- logging
- authentication
- encryption
- content security

#### 2 Run fw defaultgen.

You must ensure that your Security Policy does not interfere with the boot process.

### Verifying the Default Policy

You can verify that the default Security Policy is indeed loaded as follows:

#### 1 Boot the system.

Overview

- 2 Before installing another Security Policy, type the following command:

```
$FWDIR/bin/fw stat
```

The command's output should show that defaultfilter is installed.

## Auxiliary Connections

### Overview

A number of services establish auxiliary connections that require special handling by FireWall-1. For example, an FTP data connection from the FTP server to the client will be allowed only if the **Enable FTP PORT Data Connections** property in the **Services** tab of the **Properties Setup** window (Windows GUI) or the **Enable Response of FTP Data Connections** property in the **Control Properties/Services** window (OpenLook GUI) is enabled.

Consider the following Rule Base

Source	Destination	Services	Action	Track	Install On
FTPClient	FTPServer	Any	Accept		Gateways
Any	Any	Any	Reject	Long Log	Gateways

If the property is not enabled, the data connection from FTPServer to FTPClient will not be allowed, because there is no rule that allows connections from FTPServer to FTPClient.

If the auxiliary connection is from the client to the server (as with FTP PASV), the auxiliary connection may be improperly handled in some cases (for example, if the server's IP address is translated).

Before a back connection is opened (for example, for FTP), the back connection's destination port is checked against a list of known TCP and UDP services. If the requested port "belongs" to a well known service, the back connection is rejected.

Services that open back connections fall into two categories in FireWall-1 (assuming that there is a rule that allows the initial connection):

- FireWall-1 allows auxiliary connections only if the appropriate property is enabled.

These are:

- FTP PORT
- FTP PASV
- RSH/REXEC
- RPC Control

### Established TCP Connections

- FireWall-1 allows auxiliary connections only if the service is specifically listed under **Services** in the rule that allows the initial connection.

These are:

- |           |                                           |
|-----------|-------------------------------------------|
| ■ VDOlive | ■ WebTheatre                              |
| ■ H.323   | ■ CoolTalk                                |
| ■ BackWeb | ■ RealAudio                               |
| ■ FreeTel | ■ MS Exchange services (requires DCE-RPC) |
| ■ NetShow | ■ sqlnet2                                 |

## Established TCP Connections

### Overview

FireWall-1 inspects *all* IP packets against the Security Policy. The first packet of each TCP connection or UDP session is checked against the Rule Base. If the first packet is accepted, FireWall-1 adds the connection to an internal table of open connections (the connections table), in the format:

```
<src-addr,src-port,dst-addr,dst-port,ip-p;enc-key,type,flags>
```

Subsequent packets of an established TCP connection (or UDP session) are checked against the table rather than against the Rule Base.

FireWall-1 considers a packet to be part of an established TCP connection if it is not a SYN/NO-ACK packet, that is, if it is not the first packet of a TCP connections.

You can see the connections table by typing:

```
fw tab -t connections -u
```

on the FireWalled gateway.

One of the first things FireWall-1 does for each packet is to determine whether the packet's TCP connection (or UDP session) is listed in the connections table. If it is, the packet is immediately accepted (and possibly encrypted or decrypted).

There are several advantages to using this method:

- 1 FireWall-1 needs some way of accepting replies to valid TCP connections.

Suppose the Rule Base allows connections from A to B, but rejects connections from B to A. If A initiates a connection to B, the replies to that connection must be accepted even though connections from B to A are rejected. By using the

## Overview

connections table, FireWall-1 is able to differentiate between replies to the original A to B connection (which are allowed to pass) and B to A connections (which are rejected).

- 2 It is very inefficient to scan each packet against the entire Rule Base. It is much more efficient to accept all packets of previously approved connections.

Entries are removed from the connections table when one of the following happens:

- for TCP connections:
  - 20 to 50 seconds after FireWall-1 sees two FIN packets, or
  - after the connection is idle for more than TCP\_TIMEOUTseconds
- for UDP sessions, after the connection is idle for more than UDP\_TIMEOUT seconds

These values are set by the user in the **Security Policy** tab of the **Properties Setup** window (Windows GUI).

In addition, the connections table is cleared when a Security Policy is re-loaded (as are as most of the other tables). The new Security Policy is then enforced on the already active connections and sessions.

It may happen that an entry for a connection still taking place is removed, either because the connection was idle for a long time and has been re-activated, or because a new Security Policy was loaded.

For example, suppose your Security Policy accepts allows connections from A to B, but rejects connections from B to A. Suppose you do the following:

- 1 TELNET from A to B.
- 2 Type the command:

```
sleep 100; echo "hello"
```

- 3 Reload the same Security Policy.

After 100 seconds, a packet returns from B to A, carrying the word "hello". Although this packet is part of a valid connection, FireWall-1 rejects it.

To solve this problem, FireWall-1 drops TCP packets that claim to belong to established TCP connections (that is, non - SYN and ACK packets) in a special way. The packet is not actually dropped, but instead all the data is removed from the packet, leaving only the IP and TCP headers, which renders the packet harmless. In addition, the SEQ number of the TCP header is mangled.

When A receives the mangled packet, A immediately responds, because of the mangled SEQ number. If the connection is still valid, this response is matched against the Rule Base, and the connection is re-recorded in the connections table. If the Rule Base indicates that the connection is to be logged, then the packet is logged if Log

## Established TCP Connections

Established TCP Packets in the **Logging and Alerting** tab of the **Security Policy** window (Windows GUI) or the **Control Properties/Logging and Alerting** window (OpenLook GUI) is checked. FireWall-1 then restarts the timeout clock.

If the connection has become invalid, the packet is dropped. FireWall-1 notices that it is dropping a reply to a mangled TCP packet and so does not mangle it again but drops it for good.

In rare cases, FireWall-1 logs the mangled packets if the rule that dropped the packet specified a log action. This means that even if a connection is legal, you might see a drop log entry even though the connection continues. To eliminate these spurious log entries, uncheck **Log Established TCP Packets** in the **Logging and Alerting** tab of the **Properties Setup** window (Windows GUI) or the **Control Properties/Logging and Alerting** window (OpenLook GUI) and reload the Security Policy.

## Example

Suppose the Rule Base allows host A to initiate an FTP connection with host B, and specifies that the connection be logged. The log then shows an entry for the first packet, but not for subsequent packets (because the Rule Base is checked only for the first packet). Suppose also that the connection times out.

**If the First Packet After the Timeout is Sent by A** — If the first packet after the timeout is sent by A, it is handled as though it were the first packet of the connection. The packet is accepted and the timeout clock is restarted. If the Rule Base specifies logging, the packet is logged.

**If the First Packet After the Timeout is Sent by B** — If the first packet after the timeout is sent by B, FireWall-1 checks the Rule Base. Even if the Rule Base specifies that the packet be dropped or rejected, FireWall-1 mangles the packet and passes it to A. This forces A to request a re-transmission, upon which the Rule Base is checked again as described in "If the First Packet After the Timeout is Sent by A" above.

TABLE 12-1 summarizes the logging options for re-established TCP connections.

TABLE 12-1 Logging a Re-Established TCP Connections

Log Established TCP Packets	first packet after timeout sent by A	first packet after timeout sent by B
checked	packet is logged only if specified by Rule Base — packet is handled just as the connection's first packet was handled	packet is logged only if specified by Rule Base (possibly under last "None of the Above" rule)
not checked	packet is not logged	packet is not logged

## The Fast Mode Option

### Overview

The Fast Mode option takes advantage of the fact that all non-SYN/NO-ACK packets must be part of an established TCP connection. Therefore, a host receiving non-SYN/NO-ACK packets that are not part of an authorized session will consider these packets out of context and require the originator to properly establish the connection by sending a SYN/NO-ACK packet.

When Fast Mode is enabled for a TCP service, FireWall-1 does not enter these connections in the connections table and passes all non-SYN/NO-ACK packets, increasing the connections-per-second rate. Security is not compromised because these packets are all associated with connections already allowed by FireWall-1.

Services that open back connections (for example, FTP, VDOlive, H.323) cannot be used with Fast Mode enabled.

TABLE 12-2 lists the FireWall-1 features that cannot be used if Fast Mode is enabled.

**TABLE 12-2** FireWall-1 Features Incompatible with Fast Mode enabled

feature	reason for incompatibility
encryption	key information is stored in connections table
accounting	requires connections table

For information on how to enable Fast Mode for a TCP service, see "TCP Service Properties" on page 83 of *Managing FireWall-1 Using the Windows GUI* or "TCP Service Properties" on page 66 of *Managing FireWall-1 Using the OpenLook GUI*.

## Generic User

### Overview

If you have already defined a large number of users in an external database, you can define these users in FireWall-1 either by entering them manually or by importing them using the `fw dbimport` command (see "User Database - Importing and Exporting" on page 285). In either case, all the users will be defined and maintained in both databases.

You can avoid the burden of maintaining multiple user databases by defining a user named "generic\*" whom FireWall-1 treats in a special way. FireWall-1 applies the restrictions specified in the **User Properties** window (for example, **Allowed Sources**), but for authentication purposes, uses the name typed in by the user instead of "generic\*." In this way, the external authentication server "sees" the user's real name and authenticates him or her accordingly.



## Generic User

**Example****Definition**

For example, suppose you have already defined a large number of users to the Security Dynamics database and they are all authenticating themselves with their SecurID cards. Now, you want to integrate this authentication with FireWall-1, but you do not want to define all your SecurID users in the FireWall-1 User Database.

You can use the generic user feature as follows:

- 1 Define a user group named **SecurIDUsers** (for example).
- 2 Define a user named **generic\*** as a member of **SecurIDUsers**.
- 3 Specify **SecurID** as the **Authentication Scheme** for **generic\***.
- 4 Add a rule to the Rule Base similar to this:

Source	Destination	Services	Action	Track	Install On
SecurIDUsers@Any	tower	telnet	UserAuth	Long Log	Gateways

- 5 Install the Security Policy.



**Note** – The above rule will not be applied to users who are defined in the FireWall-1 User Database, only to users who are *not* defined in the FireWall-1 User Database.

**Using the Generic User Feature**

Suppose that Alice is a SecurID user, but she is not defined in the FireWall-1 User Database. When she TELNETs to tower (and the above rule is applied), the following sequence of events takes place:

- 1 FireWall-1 prompts Alice for her user name.
- 2 Alice enters her name.
- 3 FireWall-1 determines that Alice is an unknown user, that is, that she is *not* defined in the FireWall-1 User Database (or in any LDAP directory accessed by FireWall-1).
- 4 FireWall-1 determines that there is a user named **generic\*** defined in the User Database, whose **Authentication Method** is **SecurID**.  
  
If there is no user named **generic\***, FireWall-1 issues the "illegal user name" error message and disallows the connection.
- 5 FireWall-1 prompts Alice to enter her SecurID password.

## Notes

- 6 Alice enters her SecurID password.
- 7 FireWall-1 contacts the SecurID server and asks to authenticate user Alice, supplying the password Alice entered.
- 8 The SecurID server notifies FireWall-1 whether Alice was successfully authenticated.
- 9 FireWall-1 either allows or disallows the connection, based on whether Alice was successfully authenticated.

## Notes

- 1 By using this feature with an external server, you disable FireWall-1's ability to detect invalid user names.  
  
The responsibility of authenticating the user is passed to the external server. You will only get an alert or log if the authentication fails on the external server. Without this option, it is possible to get an alert or log when an invalid user name is entered.
- 2 By default, all the users defined in the external server are allowed access.  
  
There is no way to treat the users differently (but see item 3 below). The System Administrator should carefully consider the implications of allowing this blanket access.
- 3 If you wish to deny access to a specific user, define that user in the FireWall-1 User Database and set the user's **Authentication Scheme** to **Undefined**.
- 4 To disable this feature, delete **generic\*** from the FireWall-1 User Database, or set **generic\*'s Authentication Scheme** to **Undefined**.
- 5 This feature does not work with the S/Key and FireWall-1 Password Authentication Schemes.  
  
The user **generic\*** will always fail S/Key and FireWall-1 Password authentication, because these schemes are implemented directly by FireWall-1 and not by external servers, so their users must be defined in the FireWall-1 User Database.  
  
Nevertheless, there is still an advantage to be gained by defining a user **generic\*** with the FireWall-1 Password Authentication Scheme. An attacker who guesses at a user name will not see the error message "unknown user." Instead, the attacker will see a message indicating that the authentication failed, and will not know whether it is the name or the password that is invalid.
- 6 **generic\*** cannot be used as the name of a real user.

Redirecting Logging to Another Master

## Redirecting Logging to Another Master

### Masters and Logging Modules

A Master is a machine to which FireWall Modules direct logging. The file `$FWDIR/conf/masters` contains a list of IP addresses (or network object names), one per line. When the FireWall Module starts working, it reads this file to determine where to direct logging.

If the file `$FWDIR/conf/masters` does not exist, then the FireWall Module directs logging to the machine it is running on.

If the file `$FWDIR/conf/masters` does exist, then the FireWall Module directs logging to the first IP address in the file to which it can connect (this can also be the IP address of the local machine). If the network object has more than one interface, then the IP address given in `$FWDIR/conf/masters` should be the one facing the FireWall Module (that is, connected to the machine on which the FireWall Module is running).

If any of the IP addresses in `$FWDIR/conf/masters` is preceded by a + symbol, then logging will be directed to all the IP addresses preceded by a + symbol. In this way, it is possible to direct logging to more than one IP address at the same time. If FireWall-1 cannot connect to any of the IP addresses is preceded by a + symbol, then logging will be directed to the first IP address not preceded by a + symbol to which the FireWall Module can connect.

If the connection to the Master goes down, the FireWall Module scans `$FWDIR/conf/masters` once again, looking for an IP address to which it can connect. If it finds one, it redirects logging to that address. Otherwise, it directs logging to the machine it is running on.

### Examples

For the following `$FWDIR/conf/masters` file:

```
192.23.45.67
192.34.56.78
192.45.67.89
```

The FireWall Module will log to the first IP address in the file to which it can connect.

For the following `$FWDIR/conf/masters` file:

```
192.23.45.67
+192.45.67.89
192.34.56.78
+194.98.76.54
```

## The TCP SYN Handshake

- 1 The FireWall Module will attempt to log to both 192.45.67.89 and 194.98.76.54.
- 2 If the FireWall Module fails to connect to both these IP addresses, it will try to connect to 192.23.45.67.
- 3 If the FireWall Module fails to connect to 192.23.45.67, it will try to connect to 192.34.56.78.
- 4 If the FireWall Module also fails to connect to 192.34.56.78 (in other words, if it cannot connect to any of the IP addresses in \$FWDIR/conf/masters) it will direct logging to itself.

## The TCP SYN Flooding Attack

## The TCP SYN Handshake

TCP (Transport Control Protocol) is a connection-oriented, reliable transport protocol. Two participating hosts must first establish a connection by a three-way handshake between them. TCP assigns sequence numbers to every byte in every segment and acknowledges all data bytes received from the other end.

For example, if host A wants to establish a connection with host B, A begins by sending a SYN packet (a TCP packet with the SYN bit set) to B. B replies with a SYN/ACK packet (a TCP packet with the SYN and ACK bits set). A completes the three-way hand-shake with a TCP ACK packet.

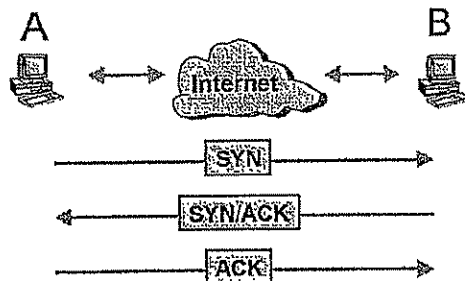


FIGURE 12-1 TCP SYN handshake

When B receives the SYN packet, it allocates substantial memory for the new connection. If there were no limit to the number of connections, a busy host would quickly exhaust all of its memory trying to process TCP connections. However, there is usually a small upper limit to the number of concurrent TCP connection requests ("backlog queue") a given application can have running on the host.

### The TCP SYN Flooding Attack

Typically, the upper limit for each server program (for example, a Web server) running on the host is ten outstanding unacknowledged (un-ACK'd) connection requests. When the backlog queue limit is reached, an attempt to establish another connection will fail until one of the backlogged connection either becomes established (SYN/ACK packet is ACK'd), is reset (a RST packet is received) or times out (usually after 75 seconds).

### How the Attack Works

The following description of a SYN flooding attack is based on an in-depth description published online in Phrack Magazine (<http://www.fc.net/phrack/files/p48/p48-13.html>).

A client initiates a TCP connection by a request with the SYN flag set in the TCP header. Normally the server replies with a SYN/ACK identified by the source IP address in the IP header. The client then sends an ACK to the server (FIGURE 12-1 on page 329) and data exchange begins.

When the client IP address is spoofed (changed) to that of an unreachable host, the targeted TCP cannot complete the three-way hand-shake and will keep trying until it times out. This is the basis for the SYN flood attack.

The attacking host (Z) sends a small number (less than 10 is sufficient) of SYN requests to the target TCP port (for example, the Web server). The attacking host also spoofs the source IP address as that of another (Z'), currently unreachable host. The process is depicted in FIGURE 12-2.

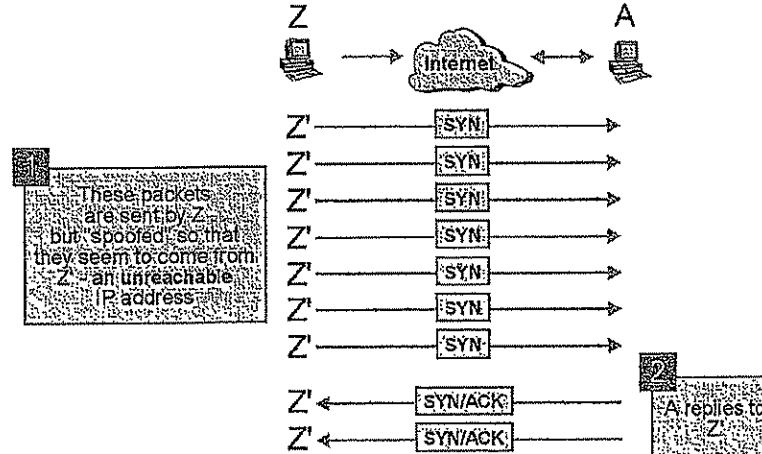


FIGURE 12-2 SYN Attack

## FireWall-1 SYNDefender

The source IP address (Z') must be unreachable because the attacker does not want any host to receive the SYN/ACKs from the target TCP, which would elicit a RST from that host (an RST packet is issued when the receiving host does not know what to do with a packet) and thus foil the attack (FIGURE 12-3).

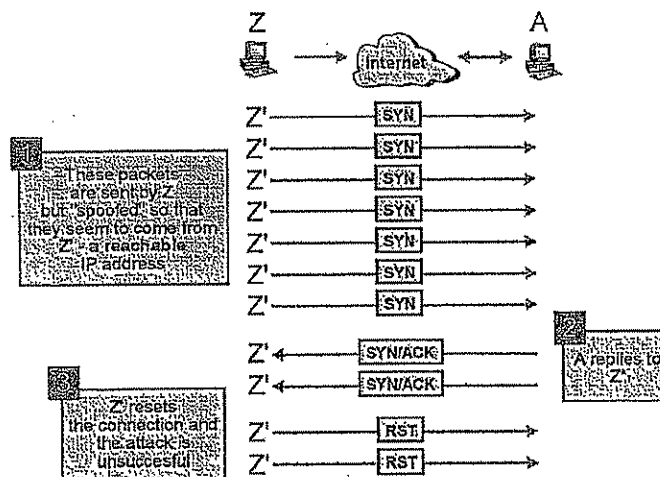


FIGURE 12-3 The SYN Attack unsuccessful, because Z' is reachable

Instead, until the SYN requests time out, A will not accept any connection requests. If the attacks were, for example, against A's Web server, then that Web server will be inaccessible for some 75 seconds as a result of an attack that lasted less than one second.

### FireWall-1 SYNDefender

Check Point's SYNDefender provides two different approaches for defending against a SYN flooding attack:

- SYNDefender Gateway
- SYNDefender Passive Gateway

All three of these solutions are integrated into the FireWall-1 Inspection Module, a high-performance kernel-level process that intercepts all packets before they are observed by the operating system and performs Stateful Inspection on these packets. The system administrator can choose which of the solutions is best suited to a particular environment.

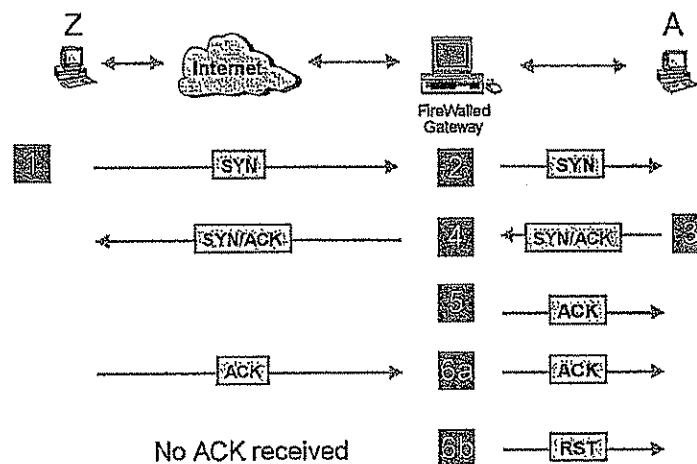
## The TCP SYN Flooding Attack

**SYNDefender Gateway**

In order for the resetting of SYN connection attempts to be effective against the SYN flooding attack, the reset timer must be short enough to keep A's backlog queue from filling up, while at the same time long enough to enable users coming over slow links to connect. The SYNDefender Gateway solution surmounts this problem by ensuring that an ACK packet is sent in immediate response to A's SYN/ACK packet.

When A receives the ACK packet, the connection is moved out of the backlog queue and becomes an open connection on A. Internet servers can typically handle hundreds or thousands of open connections, so the SYN flooding attack is no more effective in creating a denial of service condition than a hacker trying to establish an excessive number of valid connections to the server. The backlog queue is effectively kept clear and it is possible to wait longer before resetting connections which have not been completed.

SYNDefender Gateway is depicted in FIGURE 12-4.



**FIGURE 12-4** SYNDefender Gateway

- 1 FireWall-1 intercepts a SYN packet going to host A and records the event in an INPSPECT state table.
- 2 FireWall-1 lets the SYN packet continue on to A.
- 3 FireWall-1 intercept A's SYN/ACK reply to Z and correlates with the corresponding SYN packet sent by Z.
- 4 FireWall-1 lets the SYN/ACK continue on its way to Z.
- 5 FireWall-1 sends an ACK packet to A, which moves the connection out of A's backlog queue.



## FireWall-1 SYNDefender

- 6 At this point, one of two things will happen, depending on whether the connection attempt is valid.
- a If Z's connection attempt is valid, then FireWall-1 will receive an ACK from Z which it will pass on to A.
- A ignores this second redundant ACK since the three-way handshake has already been completed.
- b If Z's IP address does not exist, then no ACK packet will return from Z to A and the reset timer will expire. At this point, FireWall-1 resets the connection.

The effectiveness of the SYNDefender Gateway solution is based on quickly moving connection attempts out of the backlog queue. SYN flood connection attempts then fail to fill up the backlog queue and remain as harmless as one of the host's open connections, until the FireWall-1 timer expires and the connection is reset or canceled.

**SYNDefender Passive Gateway**

SYNDefender Passive Gateway is similar to SYNDefender Gateway, except that FireWall-1 does not simulate Z's ACK packet to A, and instead waits for Z's ACK before passing it on to A.

The unacknowledged connection remains in A's backlog table, but times out after FireWall's timeout period, which is much shorter than the backlog queue's timeout period.

FIGURE 12-5 depicts SYNDefender Passive Gateway.

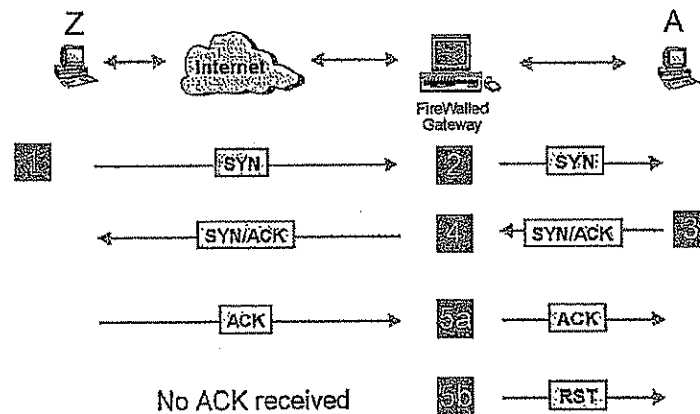


FIGURE 12-5 SYNDefender Passive Gateway

The TCP SYN Flooding Attack

### **Guidelines for Deploying SYNDefender**

While there are no strict rules for when to use each of the SYNDefender solutions, some basic guidelines will help establish the appropriate policy for a given situation.

#### **SYNDefender Gateway**

SYNDefender Gateway has two primary advantages:

- Users establishing valid connections with the protected server will not incur any delay in connection setup time.
- There is very little overhead on FireWall-1.

However, since connections are established on the server, that is, moved from the backlog queue, it is important to consider how many established connections the protected server can support relative to the normal load handled by the server.

#### **Choosing an Appropriate SYNDefender Method**

As a first step, you should consider whether you need SYNDefender at all. Since the SYN flooding attack is a "denial of service" attack rather than a security breach, it may be more effective to deploy SYNDefender only after a SYN attack actually occurs.

CHAPTER **13**

# Troubleshooting

## In This Chapter

<i>Display</i>	<i>page 335</i>
<i>Inspecting</i>	<i>page 335</i>
<i>Connectivity</i>	<i>page 340</i>
<i>Log</i>	<i>page 340</i>
<i>Installing Inspection Code</i>	<i>page 341</i>

## Display

Problems with 24-bit color displays

XView sometimes has problems with 24-bit color displays. You can work around this by specifying 8-bit color when you start the FireWall-1 GUI, as follows:

```
fwui -depth 8
```

## Inspecting

How to know what is really happening?

Use the snoop utility on Solaris 2 or Solaris i386, or etherfind on SunOS 4 or HP-UX to observe the flow of packets through an interface. On NT, use the Network Monitor.

You can connect from the gateway but not through it.

It is important to determine whether FireWall-1 is responsible, or whether the problem persists even after FireWall-1 has been stopped.

- 1 Stop the FireWall Module (fwstop).

## Inspecting

2 Determine whether the problem still exists.

3 Correct routing on the network.

If you are using Address Translation, this may be non-trivial.

4 Restart FireWall-1 (fwstart).

The system is blocked

Use the procedures in the order listed below to restore access to blocked essential services. If one procedure does not solve the problem, go on to the next one.

1 Examine the log file and determine for which services Action is Dropped or Rejected.

If an essential service is blocked, modify the Rule Base and install it again. This procedure assumes that the Rule Base logs dropped and rejected services, which is a good practice in any case.

2 Use the GUI to uninstall the Security Policy.

You may use either the Policy menu in the Rule Base Editor or the Install menu in the System Status View window.

3 Uninstall the Security Policy.

```
$FWDIR/bin/fw unload
```

4 Stop the FireWall-1 daemon and unload it from the Kernel Module by using the command:

```
$FWDIR/bin/fwstop
```

5 Kill the FireWall-1 daemon by using the following sequence of commands:

```
ps ax | grep fwd
kill <pid>
```

6 Unload the FireWall Module by using the command:

```
$FWDIR/bin/fw unload
```

- 7 Stop the system and then boot the system in single-user mode:

```
boot -s
```

- 8 After the system is booted, remove the state files of the corresponding host by typing:

```
/bin/rm $FWDIR/state/*
```



**Note** - If \$FWDIR is not defined in single user mode, then substitute the directory name.

- 9 Continue the boot process by typing ^D.

You get a message that there are too many internal hosts

This problem is usually the result of an incorrectly specified external interface (in the \$FWDIR/conf/external.if file).

When you install or upgrade FireWall-1, the installation script asks you which product you are installing. The installation procedure later asks this question:

FireWall-1 detects the number of hosts that your internal network has. In order to do it correctly, it needs to know the name of the external network interface of your gateway. You may wish to select one of the following interfaces:

```
<a neat output of ifconfig -a >.
```

If you enter a non-existent interface name, you will get the following message each time you load Inspection Code:

```
"External interface not set by this loading"
```

Then all interfaces will be considered internal and will be counted against the limit.

#### Reconfiguring the External Interface

To reconfigure the external interface, reconfigure FireWall-1 and correctly specify the interface name.

## Inspecting

Alternatively, write the name of the external interface (for example, "le1") in the (possibly non-existent) file `$FWDIR/conf/external.if`. You may wish to erase the database of internal hosts which FireWall-1 keeps in `$FWDIR/database/fwd.h` and `$FWDIR/database/fwd.hosts` (just delete the file). Next, stop FireWall-1 (`fwstop`) and restart it (`fwstart`).

If the above steps do not correct the problem, the following paragraphs describe some debugging techniques that you can use:

## Extracting the List of Internal Hosts

- 1 First, get FireWall-1's list of the internal hosts.

Check the `/var/adm/messages` file for the start of the list:

```
Jan 6 14:40:11 mutiara unix: FW-1: too many internal hosts
detected
Jan 6 14:40:11 mutiara unix: (192.100.98.167
```

and for the end of the list:

```
...
Jan 10 17:19:08 mutiara unix: FW-1: only 50 internal hosts allowed
```

- 2 Next, go through the list of hosts, as follows:

- a If all hosts are valid internal hosts, then your current license is not sufficient and you will have to upgrade to the next class (for example, from FireWall-1/50 to FireWall-1/250).

If some of the hosts have IP addresses that belong to your internal network but you don't recognize them, then ping them or telnet to them to find out if they exist.

If they don't exist, treat those hosts as unknown hosts (see "Monitoring Unknown Hosts" on page 339).

- b If all hosts are external hosts, then there are three possibilities:

- i You have specified your internal (rather than your external) interface in `$FWDIR/conf/external.if`.

Correct this error and restart FireWall-1, as above (see "Reconfiguring the External Interface" on page 337).

- ii There is another path from the external network into your internal network.

Some connections originating in the external network are coming in via that path and are coming out through the FireWalled machine. Proceed to "Monitoring Unknown Hosts" on page 339.

- iii* Someone from inside your network is trying to spoof other IP addresses.

Proceed to "Monitoring Unknown Hosts" on page 339.

### Monitoring Unknown Hosts

In order to get more information about the IP addresses that FireWall-1 is treating as internal addresses, you must log all connections. Then, for each unknown IP address in the internal host list, find the first connection with the matching IP source.

- 1** In the Rule Base Editor, choose Log under in the Track column for all rules.  
The Log will now contain detailed information for every connection.
- 2** Install the Rule Base.
- 3** Wait for the error message "too many internal hosts detected ..." to appear again.
- 4** Extract the list of internal hosts, as above (see "Extracting the List of Internal Hosts" on page 338).
- 5** Match the list against entries in the Log File.

I sometimes see the following error message:

```
fwd: fwauthd: Failed to accept: To many open files
fwd: fwauthd: pipe failed: To many open files
```

This happens when FireWall-1 runs out of file descriptors when using many concurrent encrypted connections.

The solution to the problem is as follows:

- 1** Stop FireWall-1 by typing:

```
/etc/fw/bin/fwstop
```

- 2** Add the following line to the beginning of the fwstart script (in /etc/fw/bin):

```
limit desc 1024
```



## Connectivity

### 3 Start FireWall-1 by typing:

```
fwstart
```

## Connectivity

When I bring up the user interface to login to the server, I get a message that tells me it cannot connect to the server. I have added an administrator name and password, but it does not work.

The message "cannot connect to server" is usually the result of problems in resolving the server's name to an IP address, or other network problems which prevent the GUI client from connecting to the server.

Check whether the Management Server and the GUI Client can ping each other. You can also try specifying the Management Server's IP address rather than its name in the **Server Name** field.

If the ping fails, or if using an IP address rather than a host name works, then there is a name resolution problem at the network level which is unrelated to FireWall-1.

Also, make sure that the GUI Client appears is listed in your GUI-clients file (\$FWDIR/conf/gui-clients). See "Client/Server Interaction" on page 224 for additional information.

## Log

There is nothing in the Log Viewer

- 1 Make sure the Log Viewer is not at the bottom of the log file.
- 2 Make sure the selection criteria make sense.

Try disabling them and see what happens.

Fields are truncated when printing a log

When printing a log, some of the fields, for example Src and Dst, are truncated, as in FIGURE 13-1.

Time	Action	Service	Src	Dst	Proto	S_Po	Info
19:22:40	reject	echo	www-b1.broker.ao	www.gnu.com	udp	3130	len
19:24:27	reject	echo	www-b1.broker.ao	www.gnu.com	udp	3130	len 02
19:26:12	reject	echo	www-b1.broker.ao	www.gnu.com	udp	3130	len 94
8:07:14	reject	ftp	wmxew.br.widget	www.gnu.com	tcp	1377	len 44
8:09:48	reject	ftp	wmxew.br.widget	www.gnu.com	tcp	1377	len 44

FIGURE 13-1 Log Printout Showing Truncated Fields

The values in the Log File are not truncated. The truncation takes place only when the Log File is printed.

To correct this problem, proceed as follows:

- 1 Quit all running Log Viewers.
- 2 Change the width fields in the file \$FWDIR/conf/logviewer.C from this:

```
: (Src
    :icon (src.pr)
    :color (blue)
    :width (15
        : (25)
    )
    :type (text)
    :active (1)
)
```

to this:

```
: (Src
    :icon (src.pr)
    :color (blue)
    :width (25
        : (25)
    )
    :type (text)
    :active (1)
)
```

Make the change for both Src and Dst.

- 3 To implement the changes, restart the Log Viewer.

## Installing Inspection Code

You receive a tty warning during Security Policy Install.

This warning can be safely ignored.

The Master-Client relationship became unsynchronized after FireWall-1 was re-installed.

During the installation process, you are asked to define which Masters control which Clients (FireWalled hosts). It may be that this definition was inadvertently changed when FireWall-1 was re-installed. To correct the problem, proceed as follows:

- 1 Ensure that the Master is listed in the file \$FWDIR/conf/masters on the Client side.

## Installing Inspection Code

- 2 On the Client, type:

```
fw putkey <master name> <key>
```

- 3 On the Master, type:

```
fw putkey <client name> <key>
```

- 4 Stop the FireWall Module by typing:

```
fwstop
```

- 5 Restart the FireWall Module by typing:

```
fwstart
```

A potential problem is that the Master or Client may have more than one interface and you must specify them all in the putkey command. For example, to perform a putkey on the Client to a Master with two interfaces, type:

```
fw putkey 192.34.45.33 192.34.45.34 <key>
```

CHAPTER **14**

# FAQ (Frequently Asked Questions)

## In This Chapter

<i>Installing, Upgrading and Reconfiguring</i>	<i>page 343</i>
<i>Defining Objects and Services</i>	<i>page 352</i>
<i>Daemons</i>	<i>page 355</i>
<i>Security Servers</i>	<i>page 355</i>
<i>Logging</i>	<i>page 362</i>
<i>Security</i>	<i>page 363</i>
<i>FireWall-1/n Issues</i>	<i>page 364</i>
<i>Supported Protocols and Interfaces</i>	<i>page 365</i>
<i>Inspecting</i>	<i>page 367</i>
<i>Administrative Issues</i>	<i>page 369</i>
<i>Performance</i>	<i>page 370</i>

## Installing, Upgrading and Reconfiguring

How do I move FireWall-1 to another machine?

First of all, you must ensure that you have a valid license for the new machine. Once the license issue is resolved, the simplest procedure is as follows:

- 1 Install FireWall-1 on the new machine.

If your Management Module manages FireWall Modules on other machines, you must repeat the fw putkey procedure for all the machines (see "How Can Distributed Configurations Be Managed?" on page 345).

## Installing, Upgrading and Reconfiguring

**2** Make a copy of the Security Policy files from the old machine.

For information on which files to backup, see "How do I back up my Security Policy?" on page 344.

**3** If the new machine is the FireWalled gateway, then define the new machine as a gateway.

In the new machine's **Workstation Properties** window, check the **Gateway** flag.

**4** Delete the old machine from the Network Object Manager.

Alternatively, you can leave the old machine, but uncheck the **FireWall-1 Installed** flag in its **Workstation Properties** window.

**5** Restore the Security Policy backup files (see step 2 above) to the new machine.**6** Start the GUI on the new machine to confirm that the Security Policy was successfully transferred.**7** Install the Security Policy.

The above procedure describes the simplest case: where the Management Module and FireWall Modules are on one machine, and the Security Policy is installed on gateways. If your configuration is more complicated, you will have to modify the procedure accordingly.

## How do I back up my Security Policy?

To back up your Security Policy, make copies of the following files:

**TABLE 14-1** Backing Up a Security Policy

to back up	make a copy of these files
network objects	\$FWDIR/conf/objects.C
Rule Base	<ul style="list-style-type: none"> <li>■ \$FWDIR/conf/*.W</li> <li>■ On NT and for Version 3.x on all platforms, copy \$FWDIR/conf/rulebases.fws</li> </ul>
user database	\$FWDIR/database/fwauth.NDB*

## What Objects are Carried Over from the Previous Version?

When you upgrade to a new version of FireWall-1, the installation procedure carries the following elements over to the new version:

- FireWall-1 database (users and network objects)
- Key database
- Rule Base
- Properties
- Encryption Parameters

FireWall-1 attempts to merge your database with its own new database. For example, you will have the benefit of services defined in the new version and you will retain the services you defined in the previous version. In the case of a name conflict, the old objects (the ones you defined) will be retained.

What files are modified during re-configuration?

The following files are created and/or modified during installation and reconfiguration:

- control.map
- masters
- fwauth.keys
- fwauthd.conf
- fw.license
- external.if (for FireWall-1/25, FireWall-1/50, etc.)

Must I re-install the Security Policy after upgrading?

After upgrading, FireWall-1 loses its state, so you must start the GUI and install the Security Policy.

If I change the IP address of a network object, when does the change take effect?

You must re-install the Security Policy for the change to take effect.

When you re-install a Security Policy, FireWall-1 internal state tables are cleared, so there is the possibility that some connections may be lost, as follows:

- FTP data connections
 

If you have an open FTP connection and the Security Policy is re-installed before the FTP server attempts to open the back connection, then the back connection will be rejected.
- UDP connections
- TCP connections, in very rare circumstances
- An open encrypted session will be dropped if the newly installed Security Policy allows the session to be unencrypted.

If you are concerned about losing these connections, then you should take care to re-install your Security Policy during off-peak hours.

How Can Distributed Configurations Be Managed?

How do I install or re-configure FireWall-1 when the FireWall Module and the Management Station are different machines?

## Installing, Upgrading and Reconfiguring

As an example, consider the distributed FireWall-1 configuration depicted in FIGURE 14-1.

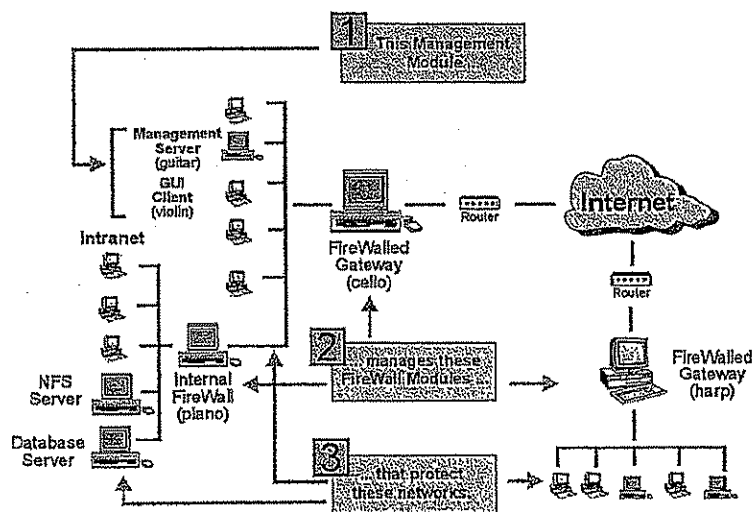


FIGURE 14-1 Distributed FireWall-1 Configuration

You must install the appropriate FireWall-1 component on each machine.

In this example, the Management Module is deployed in the Client/Server configuration, where guitar is the Management Server and violin is the GUI Client. You would install FireWall-1 as shown in TABLE 14-2.

TABLE 14-2 FireWall-1 Components

machine	FireWall-1 component
guitar	Management Module - Management Server
violin	Management Module - GUI Client
piano	FireWall Module
cello	FireWall Module
harp	FireWall Module

#### Communications within the Management Module

On guitar, the file `$FWDIR/conf/gui_clients` must list violin as one of the GUI clients authorized to use the Management Server on guitar.

For information on how and when this file is configured, see "Client/Server" on page 224.



#### Communications between the Management Module and the FireWall Modules

In this context, guitar is the Master (the repository of the Security Policy and the Log File), while cello, piano and harp are the Clients (the recipients and enforcers of the Security Policy).

When you install the FireWall-1 Management Module software, you are asked to specify the IP addresses of the remote FireWall Modules for which the Management Module is defined as Master. Conversely, when you install the FireWall-1 FireWall Module software, you are asked to specify the IP address of the Master. On the basis of this information, FireWall-1 establishes the Master-Client relationship.

The control link is the communication channel between a Master and its Clients.

On the Master and on each of the Clients, the file `$FWDIR/lib/control.map` defines access privileges and authentication measures for the control link (see "`$FWDIR/lib/control.map`" on page 348). This file is created when FireWall-1 is installed.

Communications between a Master and its Clients are authenticated according to the specifications in `$FWDIR/lib/control.map`. If the Encryption feature is installed, then communication is encrypted as well. If the Encryption feature is not installed, then communication is not encrypted.

#### Modifying an Existing Configuration

If you wish to modify an existing configuration, run `fwinstall` on all the affected machines and choose the configure option. See "Installing FireWall-1" on page 40 of *Getting Started with FireWall-1* for a description of the installation process.

Alternatively, you can reconfigure FireWall-1 by manually modifying the `$FWDIR/conf/masters` and `$FWDIR/lib/control.map` files.

To manually modify the FireWall-1 configuration, proceed as follows on each of the affected hosts (the commands given here are the Unix commands):

- 1 Stop FireWall-1 by typing `fwstop`.
- 2 Modify `$FWDIR/conf/masters` and `$FWDIR/lib/control.map`, as required.
- 3 Use the `fw putkey` command to synchronize passwords.

For information on how to use the `fw putkey` command, see "`fw putkey`" on page 261.

- 4 Start FireWall-1 by typing `fwstart`.

`$FWDIR/conf/masters`

The file `$FWDIR/conf/masters` contains a list of IP addresses (or resolvable names), one per line.

## Installing, Upgrading and Reconfiguring

FireWall-1 directs logging to the machine designated as Master, even if the Master is not itself a FireWalled gateway. For additional information, see "Redirecting Logging to Another Master" on page 327.

\$FWDIR/lib/control.map

The file \$FWDIR/lib/control.map defines access privileges and authentication measures for the control link, for example:

```
MASTERS:  stat/none    */skey
CLIENT :  load,db_download,fetch,log/fwai    */none
*:        stat/none load,unload,db_download/deny */skey
```

The entry to the left of the colon (:) can be either an IP address, a resolvable name, an asterisk (\*), a fully qualified name or the keyword "MASTERS" or "CLIENT".

On Management Stations, the allowed entries are "CLIENT", which defines how the Management Station communicates with the FireWall Modules it manages, and \*, which defines how the Management Station expects other hosts to communicate with it.

On FireWall Modules, the allowed entries are "MASTERS", which defines how the FireWall Module expects the Management Station to communicate with it, and CLIENT, which defines how the FireWall Module communicates with the Management Station.

Following the colon are strings in the following format:

```
<access> / <authentication method>
```

For example:

```
stat/none    */skey
```

means no authentication is required for status inquiries, but everything else requires S/Key authentication.

MASTERS means everything listed in \$FWDIR/conf/masters.

If the Management Station and FireWall Module define different levels of authentication, then the authentication used is the most secure of the two. For example, if the Management Station expects the FireWall Module to use fwai while the FireWall Module expects the Management Station to use S/Key, then fwai will be used. If the FireWall Module cannot use fwai (usually because the Encryption feature is not installed), then the communication will be denied.

On the Management Station, `$FWDIR/conf/masters` is empty (or doesn't exist), and `$FWDIR/lib/control.map` is the standard one created by FireWall-1 during installation.

Following is a list of access operations:

**TABLE 14-3** control.map access operations

operation	meaning
stat	status enquiry
tab_stat	get table information
get_tab_name	get table id
get_logdom	get log format or log domain
db_download	download User Database
fetch	fetch Security Policy from Master
load	load Security Policy
unload	unload Security Policy
refresh	notify daemon that a new Security Policy was installed
getkey	get public encryption key or CA key

If you have modified `control.map`, you should restart FireWall-1 (that is, run `fwstop` and then `fwstart`) in order for your modifications to take effect.

**TABLE 14-4** Authentication methods

method	meaning
none	The communication is not authenticated.
skey	The S/Key authentication method is used.
fwal	The FireWall-1 fwal authentication method is used
deny	Permission is always denied.



**Note** - `fwal` is a highly secure internal FireWall-1 authentication scheme, used primarily for encryption. If the FireWall-1 Encryption feature is not installed, `fwal` cannot be used for authentication.

## Installing, Upgrading and Reconfiguring

## Example

FIGURE 14-2 shows an example of the \$FWDIR/lib/control.map file.

```
#
# This file maps access privileges and authentication measures
# for FW's # control link.
#
MASTERS:stat,getkey,refresh/none          */fwal.
CLIENT :load,db_download,fetch,log/fwal    */none
*      :stat,getkey,refresh/none load,db_download/deny */fwal
```

**FIGURE 14-2** Example of control.map file

In this example, the line:

```
MASTERS: stat,getkey,refresh/none */fwal
```

indicates that for all the hosts listed in the file \$FWDIR/conf/masters, stat, getkey, and refresh functions are not authenticated, while all other functions are authenticated using fwal.

The line:

```
CLIENT : load,db_download,fetch,log /fwal    */none
```

indicates that this host identifies itself to its Master using the fwal authentication scheme for load, db\_download, fetch and log, but other functions do not require any authentication.

Finally, the line:

```
*      : stat,getkey,refresh/none load,db_download/deny */fwal
```

indicates that for all other hosts:

- stat, getkey and refresh require no authentication
- load and db\_download are not allowed
- all other functions require fwal authentication

### Synchronizing Authentication Passwords

The FireWall Modules on the hosts and gateways managed by a Management Station validate communication between them using an authentication password. When you install FireWall-1 on a machine, you are asked to specify an authentication password for this purpose. You must specify the same authentication password for each of the hosts and gateways managed by the same Management Station, as well as for the Management Station.

If you are re-configuring FireWall-1 manually (without using fwinstall), then you must install the authentication passwords yourself on each machine, using fw putkey. For the configuration depicted in FIGURE 14-1 on page 346, this means that you must provide the authentication passwords for three control links by performing fw putkey as follows:

**TABLE 14-5** FireWall-1 distributed configuration - fw putkey

from	to	and conversely, from	to
guitar	piano	piano	guitar
guitar	cello	cello	guitar
guitar	harp	harp	guitar

To do this, proceed as follows:

**1** Login to guitar and type:

```
fw putkey piano cello harp <key>
```

**2** Login to piano and type:

```
fw putkey guitar <key>
```

**3** Login to cello and type:

```
fw putkey guitar <key>
```

**4** Login to harp and type:

```
fw putkey guitar <key>
```

## Defining Objects and Services

Only after you have done this will the four machines be able to communicate on the control links.



**Note** – All machines must have the same name resolution for the other side. In this example, all machines must resolve guitar in the same way (to the same interface).

### "Master" and "Management Module"

The Master serves two functions:

- 1 It is the repository of the Security Policy and allows the Security Policy to be fetched by all the FireWalls for which it is defined as Master.
- 2 FireWall Modules send their log messages to the Master.

On each FireWall, the file `$FWDIR/conf/masters` contains a list of IP addresses of the machines it regards as its Masters. The FireWall Module attempts to connect to the first Master in the list; if it fails, it tries the second, and so on.

Usually, the Master and the Management Module are the same machine, that is, a FireWall's Management Module is one of the machines listed in `$FWDIR/conf/masters`. If the Management Module is the first Master in the list, then by definition, it has a copy of the Security Policy. If it is not the first Master, then when the FireWall Module needs to download its Security Policy, it will go down the list of Masters until it finds a Management Module from which it can download a Security Policy.

If for some reason you require that a FireWall Module's Management Module not be one of its Masters, then you will have to ensure that one of the Masters has an up-to-date copy of the Security Policy maintained by the Management Module.

You can direct logging to another Master, or to more than one Master. See "Redirecting Logging to Another Master" on page 327 for information on how to do this.

## Defining Objects and Services

### Which Network Objects Are on My Network?

Refer to the files `/etc/hosts` and `/etc/networks`. For Unix systems, see the manual pages for `hosts` and `networks`.

If NIS/YP (Network Information Service, formerly Sun Yellow Pages) is running on your system, use the commands `ypcat hosts` and `ypcat networks` to access network information. For Unix systems, see the manual pages for `ypcat`.

### How Do I Define the "Internet" or "Others"?

You might wish to define rules that apply to the "Internet" or to "all other hosts and networks but mine". To do that, you should first define a group network object that includes all network objects that are "mine": all your hosts, networks, domains, groups, etc.

Add the "mine" network object to the source or the destination of the rule you are defining and select it. Then use the menu options **Is Not**. This will put a cross over the "mine" network object, which indicates: any network object that **Is Not** mine (that is, not in "mine" group).

#### What's the difference between hosts, gateways and interfaces?

In defining network objects, it is important to keep in mind the distinction between hosts, gateways, and interfaces.

A gateway is a host whose **Type** is defined in the **Workstation Properties** window as **Gateway**.

A gateway will have more than one interface, but the gateway itself is a single object and should be defined as such. Each of the interfaces is defined as a separate item in the **Network Interfaces** section of the **Workstation Properties** window.

A host's name is the string returned by the `hostname` command. The IP address is the one corresponding to the host's name, as given in `/etc/hosts`, NIS/YP (Yellow Pages) or DNS.

#### Which Services and Protocols Are on My Network?

Refer to the files `/etc/services`, `/etc/rpc`, and `/etc/protocols`. For Unix systems, see the manual pages for `services`, `rpcinfo`, and `protocols`.

If NIS/YP (Network Information Service, formerly Sun Yellow Pages) is running on your system, use the commands `ypcat services` and `ypcat protocols` to access network information. For Unix systems, see the manual pages for `ypcat`.

#### Which Services Have More Than One Type?

Some services are available under more than one protocol; that is, they have more than one type. For instance, `time` and `domain` are available under both UDP and TCP; `nfs` is a UDP service and an RPC program. Some services are available under more than one protocol; that is, they have more than one type. For instance, `time` and `domain` are available under both UDP and TCP; `nfs` is a UDP service and an RPC program.

**TABLE 14-6** Services available under both TCP and UDP

service name	port number	service name	port number
chargen	19	echo	7
daytime	13	sunrpc	111
discard	9	time	37
domain	53		



## Defining Objects and Services

TABLE 14-7 Services available both as RPC and TCP or UDP

RPC name	RPC program number	TCP/UDP name	TCP/UDP number
portmapper	100000	sunrpc	UDP/TCP port 111
nfs	100003	nfs	UDP port 2049

## Which Services Are Dependent on Other Services?

Common services that require other services to function correctly are listed in TABLE 14-8 on page 354. Some services are available in several types (for instance, nfs could be UDP or RPC). Each type may have different dependencies.



**Note** – FireWall-1 is supplied with predefined service groups that ensure that access is allowed to all other services required for a service to function properly.

TABLE 14-8 Services Dependent on Other Services

Service	Type	Number	Required	Recommended
ypserv	RPC	100004	ypbind yppasswd ypupdated ypxfrd	
nfs	RPC	100003	mountd nlockmgr	ypserv
nfsd	UDP	2049	mountd	
r* (rcp, rsh but not rlogin)	commands		shell (TCP)	

## Dual DNS (Internal and External)

In a configuration that includes two Domain Name Servers (DNS) — an internal DNS for resolving internal names and an external DNS for resolving external names — the internal names can be hidden from external users by the following strategy:

- the external DNS has primary entries to a limited number of internal hosts
- the external DNS cannot issue inquiries to the internal DNS
- the internal DNS can issue inquiries to the external DNS

In this way, the internal DNS is restricted to resolving internal names for internal users while external users can gain no knowledge of internal names.

FireWall-1 can be used to enforce this strategy. The external DNS can reside on the FireWalled gateway.

#### How Many Rules Are Supported?

Theoretically, the Rule Base Editor can support a large number of rules, and Rule Bases of more than 150 rules are not uncommon. In practice, even very complex policies are normally defined in about 15 rules. Since the rules can contain group objects, a small number of rules is usually sufficient to define the Security Policy.

Is it necessary to define each of a gateway's interfaces as a separate network object? If yes, are they all gateways, or should the other interfaces be defined as hosts? Why doesn't FireWall-1 treat a gateway and all its interfaces as a single object?

The interface is not a separate network object, but rather part of another network object (gateway, router, etc.). You should *not* define interfaces as network objects. Instead, define interfaces as part of the workstation definition (on the **Interfaces** tab of the **Workstation Properties** window in the Windows GUI, or in the **Network Interfaces** section of the **Workstation Properties** window in the OpenLook GUI).

Is there a way to allow only specific ports to communicate with a system?

To limit source port number from 2000 to 3000, proceed as follows:

- 1 In the Services Manager, create a new service of type TCP or UDP.
- 2 In **Source Port Range**, enter the range 2000 - 3000.
- 3 Then use the newly created service in your Rule Base.

#### How can I control FTP from HTTP?

There is no difference, from FireWall-1's point of view, between an FTP session that originated as such (for example, a user typing ftp elvis.com) and an FTP session created when a user downloads a file by clicking on its name in a Web page. A rule that applies to one applies to the other.

If you wish to enable your users to use FTP from their Web browsers, you must define a rule allowing them to use FTP in general, without reference to HTTP. In addition, you must also:

- *not* define an FTP proxy to the browser
- set the **Enable PASV FTP Connections** property (required by some HTTP servers)

How can I restrict ping information to allow a set of machines to ping freely without restrictions, while preventing other hosts from pinging through the firewall?

Create two rules, one to allow the set of machines to send echo-requests and another to allow that same set of machines to receive echo-replies.

You can combine the two rules, either by putting both services in the same rule or by specifying "echo" (a pre-defined group which includes echo-request and echo-reply) as the service.

## Daemons

Because ping is an ICMP service and therefore has no port numbers, it is treated differently from other services, such as FTP and TELNET, which are automatically allowed to return information. The ping information is checked when it leaves and when it comes back, preventing a single rule from allowing a set of machines unrestricted pings, as the returns from the remote machines are dropped by FireWall-1.

## Daemons

inetd.conf and the Firewall-1 TELNET Daemon

*Question:* If I am running FireWall-1 with User Authentication, can I still allow a standard TELNET to the FireWalled host itself? In other words, will making a rule that allows TELNET (without User Authentication) re-install the standard in.telnetd in inetd.conf?

*Answer:* The answer to the second question is no. Once you install the FireWall-1 Security Servers, FireWall-1 modifies inetd.conf and comments out the standard TELNET and FTP daemons.

## Security Servers

How can I hide that the fact that FireWall-1 is running from users of authenticated TELNET and FTP services?

If you want users to see only the user defined message file, and not the "FireWall-1 authenticated telnet gw..." message, then add the following line to objects.C, under ":props":

```
:undo_msg (true)
```

How is FireWall-1 configured in relation to the SecurID ACE software?

The FireWall-1 software uses the standard client library of the ACE/Server. In order to use SecurID, proceed as follows:

- 1 Install and configure the ACE Server.

You will need an ACE Server somewhere in your network. The ACE Server does not have to reside on the FireWall-1 machine. For information about how to install and configure your ACE server, refer to the SecurID documentation.

- 2 In FireWall-1, create a user whose authentication scheme is SecurID.
- 3 Configure your FireWall-1 machine as an ACE Client.

The FireWall-1 software uses the standard client library of the ACE/Server. This means that you don't have to do anything special in order to integrate the software. All you have to do is to prepare the FireWalled machine as an ACE Client.

For information about how to install and configure an ACE Client, refer to the SecurID documentation.

FireWall-1 reads the `sdconf.rec` file to determine the ACE Server and other parameters involving ACE Client-Server communications. So, copy `sdconf.rec` from the ACE Server to the ACE Client.

TABLE 14-9 `sdconf.rec` directory

<code>sdconf.rec</code> directory	
Unix	<code>/var/ace</code>
Windows NT	<code>WINNT/SYSTEM32</code>

How can I define an Authentication rule for individual users rather than for groups?

The short answer is that it's not possible, but you can achieve the effect by defining a group for every user. Then you might have a user Alice and a group `GrpAlice` (with only Alice as a member), a user Bob and a group `GrpBob` (with only Bob as a member), and so on for each of your users.

The long answer is that it's not clear what the benefit of this would be, since you can define restrictions at the user level that are enforced for each user in a group. For example, suppose you have a rule like this:

Source	Destination	Services	Action	Track	Install On
<code>DayUsers@localnet</code>	Any	Any	UserAuth	Short Log	Gateways

The rule does not apply equally to all the users in the group `DayUsers`. It allows each user access only in accordance with his or her access privileges, as defined in each user's **User Properties** window. (This is true if you have chosen the default value, **Intersect with User Database**, in the rule's **User Authentication Action Properties** window.)

Suppose you want to allow Alice access only in the morning, and Bob access only in the afternoon. Just set their access privileges accordingly in their **User Properties** windows. Then, no matter which groups they belong to, they will be allowed access during those times only.

You can also set each user's **Allowed Sources** to his or her own PC. Then Alice and Bob will each be allowed access only during their defined times and only from their own PCs.

## Security Servers

On the other hand, suppose you want to restrict Alice to using only FTP and Bob to using only TELNET. Then you really do have to define separate groups, for example, GrpFTP and GrpTELNET, and define Alice as a member (perhaps the only member) of the first group and Bob as a member (perhaps the only member) of the second group, and write two rules:

Source	Destination	Services	Action	Track	Install On
GrpFTP@localnet	Any	ftp	UserAuth	Short Log	Gateways
GrpTELNET@localnet	Any	telnet	UserAuth	Short Log	Gateways

If these are the only rules in the Rule Base which apply to the members of these groups, then they will be restricted to using the given services, because the default rule will deny them access to all other services.

The interplay between the group's access privileges (as defined in the rule) and the users' access privileges (as defined in the **User Properties** window) gives you considerable flexibility.

Is it possible to authenticate FTP through a Web browser? For example, when the user tries to download a file through the Web browser, he or she should have to enter a name and password. But, when we try this, we get an error message from the browser.

When using a browser without defining a proxy in the browser, all HTTP requests use the HTTP protocol and all FTP requests use the FTP protocol. Only part of the FTP protocol is supported in this mode; only anonymous ftp requests can be performed.

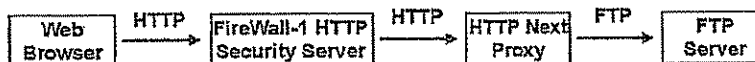
When using a browser with a proxy defined for FTP (this is defined in the browser), the defined proxy should be an HTTP proxy and not an FTP proxy. There is no way of using an FTP proxy for FTP connections when the client is a Web browser — this is a limitation of the Web browser and not of FireWall-1.

When using this configuration, the connection between the browser and the proxy uses the HTTP protocol. It is up to the proxy to convert the request from the HTTP protocol of the FTP protocol:



FIGURE 14-3 Accessing FTP through an HTTP proxy

The FireWall-1 HTTP Security Server does not support this kind of protocol conversion. So, if you wish to use the FireWall-1 to authenticate FTP requests from a Web browser, a second proxy which does support this kind of protocol conversion should be installed, and defined to FireWall-1 as the next HTTP proxy. This configuration is shown in FIGURE 14-4.



**FIGURE 14-4** Authenticating FTP through the HTTP Security Server

If you do not define a next proxy to FireWall-1, then you will get an error message "scheme ftp not supported" when you attempt to authenticate an FTP request.

For additional information, see "The HTTP Security Server in Proxy Mode" on page 49.

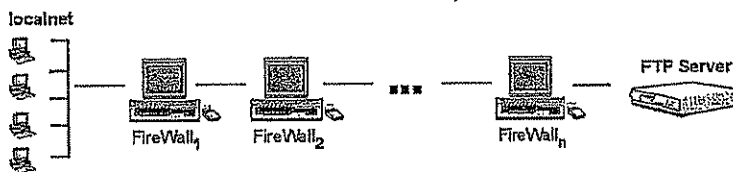
How can I go across two or more FireWalls for authenticated services?

#### TELNET

This is easy enough to do with TELNET — just TELNET to one FireWall after the other in sequence, authenticating yourself each time, until you get to your final destination.

#### FTP

For FTP, it's a little more complicated. Suppose you have  $n$  FireWalls, as in FIGURE 14-5:



**FIGURE 14-5**  $n$  FTP authenticating FireWalls

- 1 FTP to the first FireWall.
- 2 Then, as your user name, enter:
  - the user name on the FTP server and the FTP server IP address (or name), followed by
  - the user name and the IP address (or name) of the next authenticating FireWall, one after the other, separated by @ characters, in reverse order:

```

FtpUser@FtpServerIP@FW_nUser@FW_nIP@FW_{n-1}User@FW_{n-1}IP ...
@FW_2User@FW_2IP
  
```

## Security Servers

- 3 As your password, enter each password one after the other, separated by @ characters, in reverse order:

```
FtpPass@FWnPass@FWn-1Pass ... @FW1Pass
```

## HTTP

For HTTP outbound connections, just define the FireWall-1 HTTP Authenticating Server as your proxy in the browser and you will get the authentication prompts, one after the other.

If you are using a Netscape browser or Internet Explorer 3.0, then the authentication for outbound HTTP (when FireWall-1 is defined as a proxy to the browser) and inbound HTTP is done separately, that is, the user is prompted for each authentication separately, as he or she moves outward from the client.

For HTTP inbound connections, enter the list of passwords and users in reverse order. Since a password or user name can include a @ character, the passwords in the list are separated in an unusual way:

Suppose you have  $n$  FireWalls, as in FIGURE 14-6:



FIGURE 14-6  $n$  HTTP Authenticating FireWalls

After the  $n^{\text{th}}$  user enter  $2^{n-2}$  @ characters, followed by the  $n-1^{\text{th}}$  user and  $2^{n-3}$  @ characters, etc.

```
HttpUser(2n-1@)HttpServerIP@FWnUser(2n-2@)FWnIP@FWn-1User(2n-3@)FWn-1IP ... @FW2User@FW2IP
```

What happens if a user forgets the S/Key password?

Proceed as follows:

- 1 In the user's User Properties window, enter a new Secret Key (or leave it blank and let one be chosen randomly) and a Chain Length.
- 2 Click on Generate.
- 3 Click on Save Chain.

The keys are then saved to a file.



- 4 Download the User Database by choosing **Download Database** from the **Policy** menu or clicking on **DB Download** in the **Users Manager** window.

For more information, see "Database Installation" on page 79 of *Managing FireWall-1 Using the Windows GUI* or "User Database Installation" on page 61 of *Managing FireWall-1 Using the OpenLook GUI*.

The former "forgotten" keys are no longer valid, and the new keys will be used for all future authentication.

#### SMTP

When the FireWall-1 SMTP Security Server detects an error, I expect that it will notify the sender of the mail message (assuming the **Notify Sender on Error** field is checked in the SMTP Resource definition). Instead, I get a "connection to original-MTA failed" error message in the log.

This situation arises when there is no SMTP server between the sender and the FireWall Module. To understand what is happening, consider the networks in FIGURE 14-7.

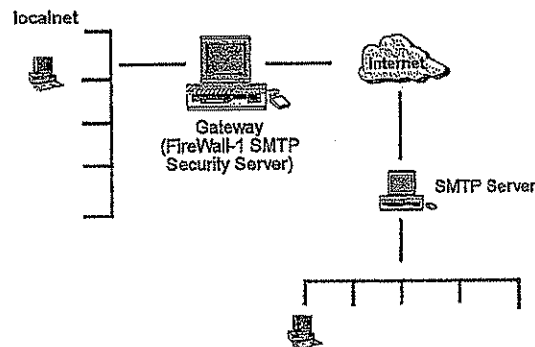


FIGURE 14-7 "connection to original-MTA failed"

Suppose a message sent from localnet is rejected by the FireWall-1 SMTP Security Server. If **Notify Sender on Error** is checked, then the Security Server will attempt to send a mail message to the original source. If that workstation is running Windows NT or Windows 95, there will usually not be a mail server listening on port 25, and the result will be the "connection to original-MTA failed" message in the log. Unix workstations usually do have mail servers installed on port 25.

On the other hand, if the original mail message arrives at the FireWall-1 SMTP Security Server from the Internet, then there will be a mail server on the return path and the notification will be successful.

In practice, this is rarely a problem, since nearly all mail messages will have passed through a mail server before arriving at the FireWall-1 SMTP Security Server.

## Logging

### Logging

#### How Can I Do a Statistical Analysis of My Log File?

Use the command `fw log` and redirect its output to a file. You can then parse the file with standard Unix tools like `perl`, `sort`, `awk`, or `sed`. Alternatively, the file can be used as input to database or spreadsheet programs.

You can also use the `fw logexport` command (see "fw logexport" on page 266) or, if you are using the Windows GUI, you can choose **Export** in the **File** menu.

Some Log entries refer to rule zero (or to rules with negative numbers!), but there are no such rules in the Rule Base.

#### Rule Zero

Rule zero is the rule FireWall-1 adds before the rules in Rule Base to implement Anti-Spoofing, dropping of packets with IP options, and some aspects of authentication. Anti-spoofing is implemented before any rules are applied, so anti-spoof track logging shows rule zero as the relevant rule.

For example, if a user fails to log in to an authentication server, then the log shows rule zero because at the time of the failure, the relevant rule (that is, the rule under which the user would have been granted or denied access had the login been successful) is unknown, since the requested service is unknown.

#### Rules with Negative Numbers

These are rules added by FireWall-1 to implement certain features. For example, a log entry generated as a result of an `fw sam` command (see "fw sam" on page 269) carries a negative rule number.

Is there any way I can choose to not log certain services? My Log File is filling up with recurring traffic through certain ports, and I don't know what these services are.

If you do not want these services to be logged, then define a rule (early in the Rule Base) that accepts them without logging them. However, from a security point of view, you should not be allowing communications unless you know what they are, so your first priority should be to identify the nature of the unknown traffic.

In my Log Viewer, I see some entries where my internal router is the Source and the protocol is ICMP. I have no idea what these entries are, or whether I should be concerned about them.

Some routers send ICMP packets from time to time, and you need not be concerned about it. You can remove the Log entries by adding a rule to the Rule Base that accepts ICMP packets from the internal router but does not log them.

How can I switch my Log File on a periodic basis?

You can do this in NT with the following command:

```
at <time> c:\winnt\fw\bin\fw logswitch
```

## Security

Does Packet Reassembly Pose a Security Risk?

FireWall-1 performs virtual packet reassembly, and does not send a packet until all its fragments have been collected. The algorithm used is stricter than the standard packet reassembly algorithm, and does not permit overlays.



**Note** – Since IP specifications forbid a router from reassembling IP fragments, FireWall-1 does not send the reassembled packet but rather the fragments as FireWall-1 received them. This is the origin of the term “Virtual Defragmentation.”

Do Aliased (or Virtual) Interfaces Pose a Security Risk?

Firewall-1 ignores virtual interfaces, so that inspection and anti-spoofing is performed on the physical interface.

If you want to use virtual interfaces with anti-spoofing, you must define two network objects, one for each subnet, and then create a network group which consists of the two network objects. Then you can put the group in the physical interface's anti-spoofing entry, just as you would if there were another physical network connected to the interface.

How does FireWall-1 prevent session hijacking?

FireWall-1's Encryption feature is the best solution, if you are concerned about this problem. Encryption would prevent hijacking by anyone who does not have the key.

How does FireWall-1 prevent attacks based on TCP sequence number prediction?

Here too, FireWall-1's Encryption feature is the best solution. Even if the attacker knows the sequence number, he or she would be unable to interfere with the encrypted connection.

How does FireWall-1 Deal with IP Options?

FireWall-1 drops packets with IP options, because they are considered to pose a serious security risk.

Is a FireWalled Host Not Secured When it Re-boots?

If IP Forwarding is disabled, then there is no time during the re-boot process during which a protected network is not secured. For further information, see “IP Forwarding” on page 275.

**FireWall-1/n issues**

For information about protecting the FireWalled host during the re-boot process, see "Default Security Policy" on page 319.

**Can FireWall-1 secure modem connections?**

FireWall-1 can secure modem connections provided that:

- the modem is "in front" of the FireWalled gateway, and
- the dial-up lines provide PPP or SLIP connections

If both these conditions are true, then FireWall-1 treats connections via the modems the same ways it treats connections via Ethernet, token ring, etc.

**FireWall-1/n Issues****How are these products restricted?**

FireWall-1/n products enforce restrictions based on the number of protected hosts. If these restrictions are exceeded, FireWall-1 will issue an error message. These restrictions are:

**1 number of internal hosts**

Up to  $n$  nodes behind the gateway are allowed, where  $n$  is the number in the product name. For example, FireWall-1/50 is restricted to 50 nodes, FireWall-1/250 is restricted to 250 nodes, etc.

A node is defined as a computing device with an IP address. A multi-user computer with one IP address is counted as one node.

This restriction relates to the number of protected hosts. Every host behind FireWall-1 is protected by FireWall-1, even if no connections to the outside are initiated from that host.

Every node protected by FireWall-1 is counted against the limit, even if its IP address is hidden from FireWall-1 by a proxy or by other means.

**2 number of external interfaces**

For all FireWall-1/n products, only one external interface may be connected to the FireWalled machine.

There is *no* restriction on the number of internal interfaces on the FireWalled machine.

**3 no external FireWall Modules**

An additional restriction for these products is that they cannot manage external FireWall Modules, that is, the Management Module and the FireWall Module must both be on the same machine. However, the Management Module can be deployed in a Client/Server configuration.



**Warning** - If you exceed the restriction on the number of protected hosts, FireWall-1 will display warning messages on the system console notifying you that you have violated the terms of the FireWall-1 license. You should *immediately* upgrade to the appropriate product in order to be in compliance with the terms of the FireWall-1 license. In the meantime, your security is not compromised and FireWall-1 will continue to protect your network.

## Supported Protocols and Interfaces

### Can FireWall-1 inspect IPX packets?

Firewall-1 completely ignores other IP level protocols, such as IPX and DecNET, which are processed by a different protocol stack. This means that if these protocol stacks are installed on the gateway they will be passed without being inspected.

Installing protocol stacks on the gateway which are not inspected by FireWall-1 is considered a security risk.

### Does FireWall-1 Support the Talk protocol?

FireWall-1 does not currently support the Talk protocol.

### Can I Use DES With ACE (SecurID)?

FireWall-1 supports the DES option of the SecurID ACE server.

### Does FireWall-1 support PPP, SLIP and X.25?

FireWall-1 supports PPP, SLIP and X.25, but these interfaces must be installed before FireWall-1 starts.

### Does FireWall-1 support Kerberos?

FireWall-1 supports the Kerberos service, but the Kerberos authentication scheme is not supported.

### Does FireWall-1 support AXENT Pathways' SecureNet Keys?

Starting with FireWall-1 Version 3.0, The FireWall-1 Security Servers support the SecureNet Keys (SNK) authentication scheme. For further information, see Chapter 1, "Authentication."

## Supported Protocols and Interfaces

## Are there any special considerations for ISDN interfaces?

If you are implementing a default Security Policy (see "Default Security Policy" on page 319) on a gateway with ISDN interfaces, FireWall-1 will not recognize the ISDN interfaces. The reason is that during the boot process, the ISDN interfaces are loaded just after the default Security Policy. When the real Security Policy is loaded, FireWall-1 "knows" that it has been loaded before, so it does not scan for new interfaces. There are several possible solutions to this problem:

- Disable the default Security Policy, at the cost of leaving the gateway exposed during the boot process.
- Deploy the default Security Policy only after the ISDN interfaces have been configured, exposing the gateway until that point.

Since the gateway is only connected to the Internet after the ISDN interfaces are configured, this solution entails a relatively short period of vulnerability.

- Leave the default Security Policy in its normal place and configure the ISDN interfaces after the real Security Policy is loaded.

In Unix systems, you will get an error message when you add the ISDN interfaces, and you must then uninstall the FireWall-1 kernel and install it, as follows:

```
fw ctl uninstall
fw ctl install
fw fetch localhost
```

For information on the fw ctl command, see "fw ctl" on page 275.

## How does FireWall-1 deal with Secure Socket Layer (SSL) and HTTPS connections?

Since all SSL negotiation, authentication and encryption take place outside the FireWall-1 software (for example, between an HTTP client and an HTTP server), FireWall-1 does not deal with SSL directly.

HTTPS is an HTTP protocol on top of SSL. The default HTTPS port number is 443, as assigned by the Internet Assigned Numbers Authority (IANA). To allow HTTPS connections, create a new service of type TCP and port number 443. Then use HTTPS in your Rule Base. For example:

Source	Destination	Services	Action	Track	Install On
localnet	Any	https	Accept	Short Log	Gateways

Note that HTTPS is not HTTP, so the FireWall-1 HTTP Authenticating Server doesn't work with HTTPS.



### How Can I Handle Multicast?

Firewall-1 does not treat multicast as a special case, so for Firewall-1, a multicast packet is simply an IP packet with a class D (224.0.0.0 — 239.255.255.255) destination address.

If you wish to specify a rule which will apply to all multicast packets, define a network object (of type network) whose IP address is 224.0.0.0 and whose netmask is 240.0.0.0. This network will encompass all legal multicast destination addresses.

To use multicast with Anti-Spoofing, add the multicast network to all the interfaces to which multicast packets might be sent. You must do this because Anti-Spoofing checks both the destination and source IP addresses.

## Inspecting

### How is a Security Policy enforced on a host's different interfaces?

A Security Policy is enforced on all the interfaces of a FireWalled host or gateway. The only way to restrict the enforcement of a rule to specific interface is by using INSPECT.

On each interface, the Security Policy is enforced differently for incoming and outgoing packets, depending on the rule's **Install On** field.



**Note** – The terms “outgoing” and “incoming” relate to the machine, not to the networks to which the machine is connected. “Incoming” means entering the machine and “outgoing” means leaving the machine, regardless of the packet's source or destination (see FIGURE 14-8)

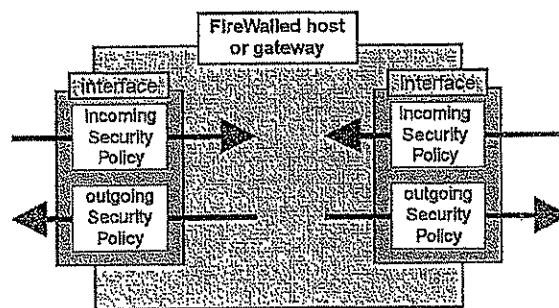


FIGURE 14-8 Incoming and Outgoing Communications



Inspecting

TABLE 14-10 describes the Security Policy enforced for FireWalled gateways. The information applies to the machines defined as **Gateways** in the **Workstation Properties** window when a rule's **Install On** field is **Gateways**.

TABLE 14-10 Gateways - Direction of Enforcement

Apply Gateway Rules to Interface Direction property	what is enforced for incoming packets	what is enforced for outgoing packets
Inbound	Rule Base and Properties	Properties (most importantly, <b>Enable Outgoing Packets</b> )
Outbound	Properties	Rule Base and Properties
Eitherbound	Rule Base and Properties	Rule Base and Properties

TABLE 14-11 describes the Security Policy enforced for FireWalled hosts. The information applies to machines defined as **Host** in the **Workstation Properties** window when a rule's **Install On** field is not **Gateways**.

TABLE 14-11 Hosts - Direction of Enforcement

Install On	what is enforced for incoming packets	what is enforced for outgoing packets
Source	Properties	Rule Base and Properties
Destination	Rule Base and Properties	Properties
Targets (host is explicitly specified)	Rule Base and Properties	Rule Base and Properties

How can I protect my internal hosts from each other?

Consider the following configuration:

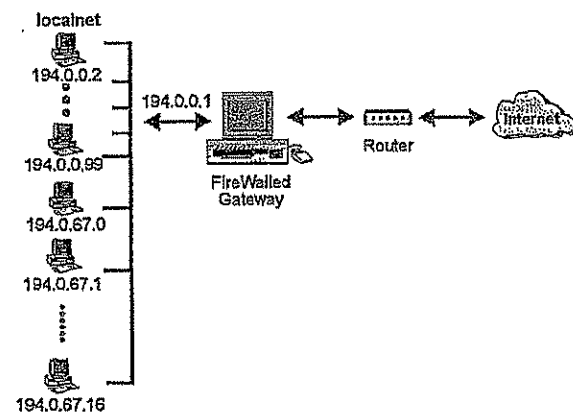


FIGURE 14-9 Protecting Internal Hosts

Assume that the Security Policy installed on the gateway does not allow TELNETs to the hosts in localnet. What happens when 194.O.O.2 TELNETs to 194.O.67.14?

The answer is that this TELNET is allowed, because the connection does not pass through the FireWall. 194.O.67.14 responds to 194.O.O.2's ARP request, and 194.O.O.2 routes the connection directly to 194.O.67.14. FireWall-1 on the gateway does not see the connection and does not inspect it.

When is a Modified Security Policy Implemented?

Changes are implemented when the Security Policy is installed. The only time it is necessary to stop FireWall-1 and restart it is after a FireWalled host's physical interfaces have changed.

How should FireWall-1 be stopped?

The correct way to stop FireWall-1 is with the `fwstop` command. If you kill the FireWall-1 daemon, the FireWall Module continues to operate, but there is no logging or authorization, and no new encryption sessions can be started.

Note that when you stop FireWall-1, your network is completely exposed. Disabling IP forwarding will protect the networks behind the gateway, but the gateway itself will still be exposed. The only way to protect the gateway in this case is to physically disconnect the network cables.

## Administrative Issues

### Security Hazards

*Question:* Are there any security hazards the administrator should be aware of when using FireWall-1?

*Answer:* FireWall-1 provides *transparent* connectivity to *all* Internet resources.

Some client-server implementations may pose security hazards, e.g., older versions of sendmail. The administrator should ensure that any application is safe to use before authorizing its use through a firewall. Since FireWall-1 enables the administrator to authorize any application, he or she has to carefully examine each one and assess the risk of allowing the use of that particular application (client or server).

### Unregistered IP Addresses

FireWall-1 enables using a large number of unregistered or concealed internal IP addresses by presenting on external traffic only a small number of registered IP addresses.

FireWall-1's Address Translation feature enables a network to use unregistered Internet addresses or to hide the internal IP addresses. For additional information, see Chapter 5, "Network Address Translation."

## Performance

### How Does FireWall-1 Address Vulnerable Applications?

To address vulnerable applications, FireWall-1 can be set up to allow inbound connections of a particular service only to a specific server that has been enhanced to handle possible failures. For example, all inbound SMTP traffic can be directed to a server running an enhanced version of sendmail. By providing such an open solution, the administrator can always acquire the latest and best application for any desired platform.

## Performance

### Does FireWall-1 Introduce Performance Degradation?

FireWall-1 introduces practically no performance degradation. Measurements conducted by several independent testers could not detect any significant decrease in network bandwidth, even at high speeds such as Ethernet and ATM. The tests were conducted by Stanford University, Open Computing magazine, Sun, and CheckPoint. The setup included standard and low-end workstations with complex security rules. At 10 Mbps the bandwidth degradation measured was about 3% and the latency was equivalent to a typical latency introduced by a gateway host.

The theoretical model developed by CheckPoint to predict performance degradation states that the impact approaches zero. This model has been empirically validated. The performance is even better at lower data rates, such as T1 or 56 kbps. For further information on this subject, refer to Rik Farrow's review in the October 1994 issue of *Open Computing*.

In contrast, encryption does have a minor but measurable impact on performance. The Accounting and Live Connection features have a more significant impact.

### What are the Guidelines for Improving FireWall-1 Performance?

#### Management Module

Installing a Security Policy on a remote FireWall Module can often be speeded up by listing both machines in the `hosts` (Unix) or `lhosts` (Windows) files.

#### FireWall Module

FireWall-1 performance depends on the hardware, the Security Policy, and the characteristics of the network traffic. While the Firewall is inspecting packets, the time of handling a packet spends in the kernel increases. The conclusion is that Firewall-1 has a greater impact on latency (connection latency or transaction latency) and less on the bandwidth.

Benchmarks have shown that, while there is usually little throughput degradation, the latency may well be significantly degraded in some cases. This degradation can as a rule, be successfully addressed. Acquiring faster hardware is always helpful. In addition, the following suggestions should improve performance as well:

**1** Keep the Rule Base simple.

Performance degrades when there is a very large number of rules, or when the rules are complex.

**2** Position the most frequently applied rules first in the Rule Base.

For example, if most connections are HTTP packets, the rule which accepts HTTP should be the first rule in the Rule Base. Be sure to keep this rule as simple as possible.

**3** Disable Accounting and Live Connections.

These features impose a significant overhead on system performance.

**4** Properties

**a** FW-1 Control Connections

This property should be disabled if possible.

**b** Enable **Fast Mode** for selected TCP services.

If you are not using Encryption, Authentication, Live Connections or Accounting, you can enable **Fast Mode** to increase the connections-per-second rate. See "The Fast Mode Option" on page 325 for more information.

**c** Decrypt on accept

This property should be disabled if you are not using Encryption or SecuRemote.

**5** Memory

If the Firewall-1 Kernel Module's memory pool is exhausted, more memory should be allocated when Firewall-1 is installed. You can find out how much memory is available by using the following command:

```
fw ctl pstat
```

More memory can be allocated as follows:

For example, suppose we want to allocate 3 Mbytes.

## Performance

**a** Stop FireWall-1 by typing:

```
fwstop
```

**i** For Solaris, add the following line to /etc/system and then reboot:

```
line set fw:fwmemem = 0x300000
```

**ii** For SunOs, type:

```
echo "fwmem ?W300000" | adb -w $FWDIR/modules/fwmod.4.1.x.o
```

**iii** For HP-UX, type:

```
echo "fwmem ?W300000" | adb -w stand/vmunix
```

**iv** For NT, set the HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\FW1\Parameters\Memory parameter in the Registry to the desired value.

**Caution** - Setting the above parameter to too high a value may hang the machine during the boot process.

**b** Restart FireWall-1 by typing:

```
fwstart
```

**6** Overhead

Logging, Accounting, Encryption, Live Connections, Network Address Translation and Security Servers all degrade performance to some extent.

Logging, Accounting and Security Servers add I/O overhead and context switches. The degradation in performance might be significant if they are used in frequently applied rules.

How can I estimate FireWall-1's memory usage?

For the FireWall Module, you can use the following general guidelines:

- Each session requires about 120 bytes of memory, more if the session is authenticated or if address translation is used.

- In addition, there is some static overhead as well.
- The FireWall Module does not release the memory used by a session until about 50 seconds after the session ends, so if there are many sessions significantly shorter than a minute, the FireWall Module needs more memory than the number of active sessions would indicate.
- For HTTP, each URL access is a separate session.

The general formula is:

$$\text{MemoryUsage} = ((\text{ConcurrentConnections}) / (\text{AverageLifetime})) * (\text{AverageLifetime} + 50 \text{ seconds}) * 120$$

#### To What Extent is FireWall-1 Fault Tolerant?

The FireWall-1 FireWall Modules will continue inspecting and reporting logs, alerts, and status even if the Master is not active for any reason (host went down, application exited, etc.). Users can define multiple default Masters to which the FireWall Modules will report logs, alerts, and status in the event that the first Master is unavailable. The status and statistics of FireWall Modules can be monitored constantly by a number of Management Stations or SNMP platforms. If the FireWall Module host is rebooted, the FireWall Module can be loaded automatically and brought up with the latest Security Policy installed. The FireWall Module can also be configured to fetch its Security Policy from various Management Stations every time it boots.

The SNMP daemon is used to report status and even if it dies, the only thing that would happen is that in FireWall-1's Status Window or on the SNMP platform, the user would see that it is no longer possible to communicate with the daemon.

The FireWall-1 daemon (fwd) is used to control the FireWall Module. If it dies, the user would not be able to control it, but the FireWall Module would continue to enforce the Security Policy that was last loaded.

As long as a gateway is up and routing, all packets are subject to FireWall-1's FireWall Module inspection. If the gateway reboots, FireWall-1's FireWall Module is immediately loaded into the kernel and the latest Security Policy is loaded into it and enforced. FireWall-1 can be configured so that IP Forwarding is enabled only when the Security Policy is being enforced (see "IP Forwarding" on page 275 for additional information).

The FireWall-1 FireWall Module keeps a local copy of the latest Security Policy, so that even if the Management Station is down when the gateway reboots, the FireWall Module will still load the latest Security Policy.

With respect to logging, the FireWall-1 FireWall Module can be configured to send logs and alerts to a certain host (the Master). If the Master is not available, the FireWall-1 FireWall Module can be configured to attempt logging to another host, and another and another. Even if logging fails, the FireWall Module will still continue to function.

Performance

374 FireWall-1 Architecture and Administration • September 1998



CHAPTER **15**

# Directories and Files

## FireWall-1 directories

TABLE 15-1 FireWall-1 directories

Directory	Description	Described on
bin	executable files	page 376
cisco	Cisco routers' executable files (Unix only)	page 377
conf	GUI configuration and files	page 377
database	on FireWalled hosts, holds temporary copy of FireWall-1 database	page 379
doc	documentation and help files (Unix only)	page 380
lib	FireWall-1 language library files	page 380
log	log files	page 383
man	man pages (Unix only)	page 383
modules	Inspection Code module files	page 383
state	state files for hosts	page 384
tmp	temporary files (compilations and internal) and pid (process ID number)	page 384
well	Wellfleet routers' executable and configuration files (Unix only)	page 385



**Note** – In Windows, the Install application writes the DeIs11.isu file in the \$FWDIR directory, for use by the Uninstaller.

**bin directory**

TABLE 15-2 bin directory

File	Description
alert.exe	(NT)
cpp	C pre-processor
display.bat	NT only
fw	command line executable
fwalert	executable for alert action
fwav	CVP server executable
fwavstart	start script for CVP server
fwavstop	stop script for CVP server
fwc	FireWall-1 compilation script
fwinfo	
fwinfo.pmr	NT Performance Monitor file
fwinfo2	
fwcisco -> ../ cisco/fwcisco	link to router command line executable
fwciscoload	executable for downloading Access List to Cisco router
fwcmsd.exe	
fwcomp	FireWall-1 language compiler
fwconfig	FireWall-1 configuration
fwd	daemon
fwell	executable for Wellfleet routers, using SNMP
fwinfo	generate debug information regarding the FireWall-1 configuration
fwinstall	software installation and configuration script
fwlv	GUI Log Viewer
fwm	Management Server for Unix and Windows GUI Clients
fwsgui	sample Session Authentication agent executable
fwstart	start script: load module, start daemons, and install Inspection Code
fwstop	stop script: kill daemons, unload module
fwui	FireWall-1 GUI
fwuninstall	FireWall-1 software un-installation script
fwuninst	FireWall-1 software un-installation executable (NT)

cisco directory

TABLE 15-2 bin directory (continued)

File	Description
fwxauth	Pops up an authentication window for use with the x11-verify service, but note that Session Authentication with <b>Contact Agent At set to Destination</b> (see "Session Authentication" in Chapter 1, "Authentication" of <i>FireWall-1 Architecture and Administration</i> ) is recommended for this kind of authentication. (Unix only)
fwxlcconf	Address Translation configuration executable
gunzip	GNU uncompression executable
in.aclntd	Client Authentication daemon
in.aftpd	FTP Security Server
in.ahttpd	HTTP Security Server
in.arlogind	RLOGIN Security Server
in.asnmpd	SMTP Security Server
in.telnetd	TelNET Security Server
in.lhttpd	Security Server
load_agent	Load Measuring Agent ("Load Measuring" on page 239)
router_load.exe	
sendmail.exe	
snmp_trap	SNMP trap executable
snmpd	FireWall-1 SNMP daemon
status_alert	status_alert executable
VIRSIG.DAT	Cheyenne virus signature file

**cisco directory**

TABLE 15-3 cisco directory

File	Description
fwciscoload	executable for downloading Access List to Cisco router

**conf directory**

TABLE 15-4 conf directory

File	Description
*.C	configuration file
*.W	Rule Base
auth.C	
clients	

TABLE 15-4 conf directory (continued)

File	Description										
default.W	default rule-base in FireWall-1 GUI format										
dnsinfo	DNS configuration file for SecuRemote (see "DNS" on page 97 of <i>Virtual Private Networking with FireWall-1</i> )										
external.if	used by the restricted versions of FireWall-1 — specifies the name of the external interface (for example, "leO" or "EPRO1") on which IP addresses should not be counted against the limit										
fwauth.NDB	user database — not a text file										
fwauth.NDB7											
fwauth.NDBBKP	user database backup file										
fwauthd.conf	created during installation process; corresponds to inetd.conf (see "Security Server Configuration" in Chapter 2, "Security Servers" of <i>FireWall-1 Architecture and Administration</i> ). During the installation process, the original telnet and ftp are commented out in inetd.conf.										
fwauth.keys	internal S/Key authentication file										
fwav.conf	configuration file for Anti Virus CVP server included with FireWall-1										
fwusers	<p>list of FireWall-1 administrators Each line is in the format: <i>name encrypted-password permission</i> where <i>permission</i> is one of the following:</p> <table> <tr> <th>value</th><th>meaning</th></tr> <tr> <td>40000000</td><td>monitor</td></tr> <tr> <td>00000000</td><td>read</td></tr> <tr> <td>01010101</td><td>read-write</td></tr> <tr> <td>00000100</td><td>user</td></tr> </table>	value	meaning	40000000	monitor	00000000	read	01010101	read-write	00000100	user
value	meaning										
40000000	monitor										
00000000	read										
01010101	read-write										
00000100	user										
fwopsec.conf	OPSEC configuration file. See the FireWall-1 OPSEC documentation for more information.										
fwrl.conf											
gui-clients	A list of IP addresses (or network object names), one per line, from which GUI Clients may attach to the Management Server										
serverkeys.*	internal S/Key authentication files										
logviewer.C	Log Viewer GUI objects and layout file										
masters	A list of IP addresses (or network object names), one per line. When the FireWall Module starts working, it reads this file to determine where to direct logging. The network objects listed in this file are also those which are allowed to load FireWall Modules to this machine.										
objects.C	FireWall-1 GUI objects and layout file										

conf/lists directory

TABLE 15-4 conf directory (continued)

File	Description
omd.conf	
options.conf	FireWall-1 product names (for installation)
product.conf	FireWall-1 installed product and options. You should not modify this file.
rulebases.fws	combined Rule Bases for Windows GUI
slapd.conf	
snmp.C	FireWall-1 snmpd configuration file (see Chapter 9, "SNMP and Network Management Tools" of <i>FireWall-1 Architecture and Administration</i> )
smtp.conf	SMTP Security Server configuration file (see FIGURE 2-5 on page 110 of <i>FireWall-1 Architecture and Administration</i> )
smtp.conf.org	
Standard.W	
trapexec.conf	list of programs FireWall-1 kernel module can run
xlate.conf	Address Translation configuration file

**conf/lists directory**

This directory contains URL lists.

**conf/ahclientd directory**

This directory contains HTML files used by the Client Authentication daemon (aclntd).

**database directory**

This directory is on the FireWalled machine, and its files are part of the Security Policy.

TABLE 15-5 database directory

File	Description
authkeys.C	maintained by the local FireWall daemon
rules.C	Rule Base - authentication rules
fwauth.NDB	user database - not a text file
fwuserauth.NDB	user authentication user database - not a text file
objects.C	downloaded from Management Module

## doc directory

This directory is for Unix only.

TABLE 15-6 doc directory

File	Description
fw.info	GUI FireWall-1 on-line help text
fwlv.info	GUI Log Viewer on-line help text

## database/lists directory

This directory contains URL lists.

## lib directory

TABLE 15-7 lib directory

File	Description
*.def	INSPECT include files
*.h	INSPECT include files
auth.def	Rule Base header definitions include file (authentication)
base.def	FireWall-1 language aliases, routines and macro definitions
code.def	header definitions include file
control.map	maps access privileges and authentication measures for FireWall-1's control link (see "How Can Distributed Configurations Be Managed?" in Chapter 14, "FAQ (Frequently Asked Questions)" of <i>FireWall-1 Architecture and Administration</i> )
crypt.def	encryption header definitions include file
defaultfilter.drop	default "drop" Security Policy
default.pf	default Security Policy
defaultfilter.boot	default "boot" Security Policy
dup.def	debugging header definitions include file
eht_set.C	settings for HTML weeding
formats.def	log format header definitions include file
fwconn.h	structure of the connections table
fwctrnm.h	
fwctrs.h	(NT only) strings for NT Performance Monitor
fwctrs.ini	(NT only) strings for NT Performance Monitor
fwf2htbin.gif	
fwf2htdir.gif	
fwf2htunknown.gif	

lib/ldap directory

TABLE 15-7 lib directory (continued)

File	Description
fwntperf.dll	(NT only) FireWall-1 Performance Monitor DLL
fwsnmp.dll	(NT only) FireWall-1 SNMP agent DLL
fwui_head.def	Rule Base header definitions include file
fwui_trail.def	Rule Base trailing definitions — last "drop everything" rule
gps.pro	Postscript log printint prologue
init.def	
kertabs.def	kernel table definitions
kerntabs.h	
libsun_av.so	Unix only
setup.C	GUI menus setup file
snmp	SNMP configuration files sub-directory
snmp.def	snmp definition headers
std.def	FireWall-1 command line aliases, routines and macros
table.def	table definitions include file
tcpip.def	FireWall-1 definitions of TCP/IP
traps.def	traps definitions include file
traps.h	traps include file
user.def	site specific INSPECT definitions
wellfleet.C	for Bay Networks routers
xtreme.def	protocol definitions include file

**lib/ldap directory**

This directory is for NT only.

TABLE 15-8 lib/ldap directory

File	Description
schema.ldif	FireWall-1 LDAP schema



### lib/snmp directory

For additional information about the FireWall-1 MIB, see "Firewall-1 MIB" on page 242.

**TABLE 15-9** lib/snmp directory

File	Description
chkpnt.mib	FireWall-1 MIB — contains variable definitions for Firewall-1's SNMP daemon; can be used to incorporate the Check Point MIB into any MIB browser or network management system.
mib.txt	FireWall-1 MIB — accessed by the FireWall-1 SNMP daemon (snmpd).
mib.txt2	FireWall-1 MIB — compatible with SNMP managers such as SunNetManager.
wellfleet.mib	from Bay Networks

# **EXHIBIT 3**

## **PART 6**

log directory

**log directory****TABLE 15-10** log directory

File	Description
	FireWall-1 old Log File; name is date log was switched
*.pid	FireWall-1 processes process id number, used by fwstop and fw kill
aSERVERNAME.log	
fw.*alog	FireWall-1 current Accounting Log File
fw.*alogptr	pointers to fw.*alog
fw.*log	FireWall-1 current Log File
fw.*logptr	pointers to fw.log
fw.logtrack	a list of log files and unique identifying numbers (based on inode or timestamp)
fw.*vlog	FireWall-1 current Active (Live) Connections Log File
fw.*vlogptr	pointers to fw.*vlog
fwui.log	a text file log of FireWall-1 GUI Client events
manage.lock	lock file — This file is created by the Windows GUI Client or by fwm on behalf of a Unix GUI Client and is used to prevent two GUI Clients from simultaneously modifying a Security Policy. It contains the name of the locking process and other identifying information. The file is deleted by the process that created it when that process terminates normally.

In NT only, the files fw.log, fw.alog and fw.vlog are not the real Log Files, but only pointers to the real Log Files (fw.log0, fw.alog0 and fw.vlog0). This mechanism enables Log Files to be purged and renamed while they appear to be open.

**man directory**

This directory is present in Unix only, and holds the man pages.

**modules directory****TABLE 15-11** modules directory

File	Description
fw.conf	kernel configuration file (Unix only)
fw.mkdev	(Unix only)
fw.sys	(NT only) the FireWall-1 driver which is copied to ..\System32\Drivers (In NT 4.0 this file is copied to two different locations)
fwmod.*	kernel modules (Unix only)

## state directory

The names of the files in this directory depend on whether the machine is a Master or a FireWalled host. If the machine is a Master, then there is a set of the files listed below for each of the managed hosts. In each set, the file names correspond to the host names.

If the machine is a managed host, then there is only one set of files, and the file names are `hostname.*`.

For example, if a Master named `elvis` manages hosts `lisa` and `marie`, then on `elvis` there would be two sets of files: `lisa.*` and `marie.*`. On `lisa`, there is a set of files named `lisa.*`, and on `marie` there is a set of files named `marie.*`.

TABLE 15-12 state directory

File	Description
<code>default.bin</code>	default filter
<code>fwrlconf</code>	loading configuration file
<code>hostname.ctlver</code>	the Management Module version that created the current Security Policy
<code>hostname.db</code>	users/encryption database
<code>hostname.fc</code>	last filter code file for host <i>hostname</i>
<code>hostname.ft</code>	last filter tables file for host <i>hostname</i>
<code>hostname.ifs</code>	last state of "myhost": Filter name and interfaces
<code>hostname.lg</code>	last filter log and alert formats for <i>hostname</i>
<code>hostname.objects</code>	network objects database
<code>hostname.set</code>	portions of Rule Base (.W)
<code>local.arp</code>	Establishes correspondence between IP addresses and MAC addresses for NT (see "From the Outside" on page 166 for an example of when this file is needed).

## tmp directory

TABLE 15-13 tmp directory

File	Description
<code>default.fc</code>	filter code (assembler) compiled from <code>default.pf</code>
<code>default.ft</code>	tables file derived from <code>default.pf</code>
<code>default.lg</code>	filter log and alert formats derived from <code>default.pf</code>
<code>fwd.pid</code>	
<code>fwm.pid</code>	
<code>slapd.pid</code>	

well directory

**well directory**

This directory is for Unix only.

**TABLE 15-14** well directory

File	Description
<code>fwll -&gt; ../bin/ fwll</code>	see "bin directory" on page 376
<code>wellfleet.C</code>	configuration file
<code>wellfleet.mib</code>	SNMP MIB describing interaction between FireWall-1 and Bay Networks routers

386 FireWall-1 Architecture and Administration • September 1998

CHAPTER **16**

# Services

## In This Chapter

<i>TCP Services</i>	<i>page 387</i>
<i>UDP Services</i>	<i>page 393</i>
<i>RPC Services</i>	<i>page 397</i>
<i>ICMP Services</i>	<i>page 398</i>
<i>Other IP Protocol Services</i>	<i>page 399</i>

## TCP Services

TABLE 16-1 TCP Services

Service Name	normal port number	Description	pre-defined in FireWall-1	Comments
AOL (America OnLine)	5190	protocol used by AOL clients to connect to AOL through a network connection, as opposed to a dial-up connection	Yes	
chargen	19	A TCP chargen server sends an unending stream of characters until the client terminates the connection.	No	This is also a UDP service.
Connected OnLine Backup	16384	PC agents that wake up occasionally and back up their encrypted data to the Connected backup server across the Internet.	Yes	

387



## TCP Services

TABLE 16-1 TCP Services (continued)

Service Name	normal port number	Description	pre-defined in FireWall-1	Comments
Cooltalk	6499, 6500	a voice communication protocol	Yes	To enable auxiliary (back) data connections for this service, you must specifically list this service under <b>Services</b> in the Rule Base. UDP is used for the voice connection.
daytime	13	A daytime server returns date and time of day in text format.	Yes	This is also a UDP service.
discard	9	A discard server discards whatever it is sent by a client.	Yes	This is also a UDP service.
DNS	53	Domain Name System — a distributed database used to map host names to IP addresses	Yes	This is also a UDP service. TCP DNS is used for Domain Name Download, while UDP DNS is used for Domain Name Queries.
echo	7	An echo server sends the client whatever the client sent the server.	Yes	This is also a UDP service.
exec	512		Yes	see "rexec" on page 391
finger	79	a protocol that provides information about users on a specified host	Yes	
ftp	21	File Transfer Protocol — a protocol for copying files between hosts	Yes	To enable auxiliary data connections, check <b>Enable FTP PORT Data Connections</b> in the <b>Services</b> tab of the <b>Properties Setup</b> window.
gopher	70	a menu driven front end to other Internet services, such as Archie, anonymous FTP and WAIS	Yes	
http	80	HyperText Transfer Protocol — a protocol used to implement the World Wide Web	Yes	
https	443	a version of HTTP that uses SSL for encryption	Yes	

TABLE 16-1 TCP Services (continued)

Service Name	normal port number	Description	pre-defined in FireWall-1	Comments
H.323	1720	client-to-client audio-visual application	Yes	To enable auxiliary (back) data connections for this service, you must specifically list this service under <b>Services</b> in the Rule Base.  ■ H.225 static connection sets up H.245 dynamic connection on dynamic TCP port, which opens two dynamic UDP connections with successive port numbers (that is, if first connection ports are A and B then second connection uses A+1 and B+1).  ■ NAT Support
ident	113	a protocol used for user identification	Yes	
imap	143	Internet Mail Access Protocol	Yes	
irc	6670, 6680	Internet Relay Chat — a protocol for on-line "chat" conversations over the Internet	Yes	
kerberos	750	an authentication service	Yes	as <i>Kerberos</i> This is also a UDP service. The Kerberos authentication scheme is not supported by FireWall-1.
ldap	389	Lightweight Directory Access Protocol (simple X500 protocol).	Yes	
ldap-ssl	636	Lightweight Directory Access Protocol over SSL.	Yes	
LiveLan	1720	H.323 based applications such as LiveLAN	Yes	see "H.323" on page 389
login	513		Yes	see "rlogin" on page 391
Lotus Notes	1352	a proprietary protocol developed by Lotus to implement its Notes application	Yes	
Microsoft Conferencing		a voice conferencing and remote application sharing protocol	Yes	

## TCP Services

TABLE 16-1 TCP Services (continued)

Service Name	normal port number	Description	pre-defined in Firewall-1	Comments
Microsoft Exchange		messaging center (mail, news, users directory)	Yes	To enable auxiliary data connections for this service, you must specifically list this service under <b>Services</b> in the Rule Base.  ■ The client requests service on DCE-RPC mapper (port 135), then initiates TCP connection to port it received from mapper. ■ experimental support ■ You must specifically allow DCE-RPC under <b>Services</b> in the Rule Base.
Microsoft NetMeeting	1503	voice communication (one to one or conference) and application sharing over the Internet	Yes	Uses H.323.
Microsoft NetShow	1755	streaming client-server multimedia	Yes	To enable auxiliary data connections for this service, you must specifically list this service under <b>Services</b> in the Rule Base.  ■ The client sends port command to server, and the server starts UDP on that port to the client. ■ NAT support
Microsoft SQL Server 5.0	1433	a data replication server	Yes	
Mosaic			Yes	a group consisting ofarchie, ftp, gopher and http
nbssession	139		Yes	belongs to the NBT group
NBT		A NetBIOS extension defining an expanded application interface	Yes	
netstat	15		Yes	
nntp	119	a protocol used to transmit news	Yes	

TABLE 16-1 TCP Services (continued)

Service Name	normal port number	Description	pre-defined in Firewall-1	Comments
ntp	123	time protocol with synchronization — a protocol providing access over to Internet to systems with precise clocks	Yes	This is also a UDP service.
Open Windows	2000		Yes	
PointCast	80	a protocol for viewing news in TV like fashion	No	
pop2	109	Post Office Protocol — a mail protocol that allows a remote mail client to read mail from a server	Yes	
pop3	110	Post Office Protocol — a modified version of pop2	Yes	
RAS		Remote Access Service	Yes	
RealAudio	7070	a protocol for the transmission of high quality sound on the Internet	Yes	To enable auxiliary (back) data connections for this service, you must specifically list this service under <b>Services</b> in the Rule Base.
rexec	512	a protocol that provides remote execution facilities with authentication	Yes	as <i>exec</i> To enable stderr, check <b>Enable RSH/REXEC Reverse stderr Connections</b> in the <b>Services</b> tab of the <b>Properties Setup</b> window.
rlogin	513	remote login — a protocol that enables remote login between hosts	Yes	as <i>login</i> To enable stderr, check <b>Enable RSH/REXEC Reverse stderr Connections</b> in the <b>Services</b> tab of the <b>Properties Setup</b> window.
rsh	514	remote shell — a protocol that allows commands to be executed on another system	Yes	as <i>shell</i> To enable stderr, check <b>Enable RSH/REXEC Reverse stderr Connections</b> in the <b>Services</b> tab of the <b>Properties Setup</b> window.
SecurID		a protocol used by an authentication service product of Security Dynamics Technologies, Inc.	Yes	SecurID is a group consisting of the services required to implement SecurID.
securidprop	5510	a SecurID service	Yes	

## TCP Services

TABLE 16-1 TCP Services (continued)

Service Name	normal port number	Description	pre-defined in Firewall-1	Comments
smtp	25	Simple Mail Transfer Protocol — a protocol widely used for the transmission of e-mail	Yes	
SQLNet	1521, 1525	an Oracle protocol for transmission of SQL queries	Yes	<p>To enable auxiliary data connections for this service, you must specifically list this service under <b>Services</b> in the Rule Base. This service can work in two modes:</p> <ul style="list-style-type: none"> <li>■ In the first, the client connects to the server using TCP port 1521.</li> <li>■ In the second, the client connects to a manager server on TGP 1521 or 1525. This server sends the client a new server IP and port, then the client connects to the new server.</li> </ul>
Sybase SQL	> 1024	client-server database	No	uses a static TCP port (defined in the Sybase setup) above 1024
TACACS+	49	an authentication protocol	Yes	as <i>TACACSplus</i>
telnet	23	Telecommunications Network Protocol — a remote terminal protocol enabling any terminal to login to any host	Yes	
time	37	a service that returns the time of day as a binary number	Yes	This is also a UDP service.
uucp	540	Unix to Unix Copy	Yes	
Vosaic	1235	audio and video based on VDP (Video Datagram Protocol)	Yes	also uses UDP ports 61801-61821
VDO-Live	7000	a protocol for the transmission of high quality video on the Internet	Yes	To enable auxiliary (back) data connections for this service, you must specifically list this service under <b>Services</b> in the Rule Base.
wais	210	Wide Area Information Servers — a tool for keyword searches, based on database content, of databases on the Internet	Yes	

TABLE 16-1 TCP Services (continued)

Service Name	normal port number	Description	pre-defined in Firewall-1	Comments
Webtheatre	12468	live audio & video streaming	Yes	<p>To enable auxiliary data connections for this service, you must specifically list this service under <b>Services</b> in the Rule Base.</p> <ul style="list-style-type: none"> <li>■ Client opens TCP port 12468 by default for control. For each media stream request there is a port command from client to server including the RTP (UDP) port the client is waiting on. The audio passes on the RTP port and the control on the RTCP port (RTCP port = RTP port + 1).</li> <li>■ NAT support</li> </ul>
WinFrame	1494	remote LAN access	Yes	
X11	6000 – 6063	a windowing system protocol	Yes	

## UDP Services

TABLE 16-2 UDP Services

Service Name	normal port number	Description	pre-defined in Firewall-1	Comments
archie	1525	a tool for keyword searches, based on file names, of files on the Internet available through FTP	Yes	
BackWeb	370	a UDP service similar to PointCast	Yes	<p>source port 371</p> <p>To enable auxiliary data connections for this service, you must specifically list this service under <b>Services</b> in the Rule Base.</p>
biff	512		Yes	

## UDP Services

TABLE 16-2 UDP Services (continued)

Service Name	normal port number	Description	pre-defined in Firewall-1	Comments
bootp	67	Bootstrap Protocol — a protocol for booting diskless systems	Yes	
chargen	19	A UDP chargen server sends a datagram containing a random number of characters in response to each datagram sent by a client.	No	This is also a TCP service.
CU-SeeMe	7648 – 7652	video, audio and chat (client to client); needs video camera	Yes	
daytime	13	A daytime server returns date and time of day in text format.	Yes	This is also a TCP service.
discard	9	A discard server discards whatever it is sent by a client.	Yes	This is also a TCP service.
dns	53	Domain Name System — a distributed database used to map host names to IP addresses	Yes	This is also a TCP service. TCP DNS is used for Domain Name Download, while UDP DNS is used for Domain Name Queries.
echo	7	An echo server sends the client whatever the client sent the server.	Yes	This is also a TCP service.
FreeTel	21300, 21301	a voice communication protocol	Yes	To enable auxiliary data connections for this service, you must specifically list this service under Services in the Rule Base.
InternetPhone	22555	a protocol for the transmission of voice quality sound over the Internet	Yes	
ISAKMP	500	an encryption protocol	Yes	
kerberos	750	an authentication service	Yes	This is also a TCP service. The Kerberos authentication scheme is <i>not</i> supported by Firewall-1.
name	42		Yes	
nbdatalogram	138		Yes	belongs to the NET group
nbname	137		Yes	belongs to the NET group
nfsd	2049		Yes	belongs to the NFS group



TABLE 16-2 UDP Services (continued)

Service Name	normal port number	Description	pre-defined in FireWall-1	Comments
ntp	123	time protocol with synchronization — a protocol providing access over to Internet to systems with precise clocks	Yes	This is also a TCP service.
OnTime	1622	client/server calendar services	Yes	
RADIUS	1645	an authentication protocol	Yes	
RAS		Remote Access Service	Yes	
RDP	259	an internal FireWall-1 protocol used for establishing encrypted sessions	Yes	
rip	520	Routing Information Protocol — a protocol used to implement dynamic routing	Yes	
SecurID		a protocol used by an authentication service product of Security Dynamics Technologies, Inc.	Yes	SecurID is a group consisting of the services required to implement SecurID.
securid-udp	5510	a SecurID service	Yes	
snmp	161	a protocol used for managing network resources	Yes	See also Chapter 9, "SNMP and Network Management Tools".
snmp-read	161	read only snmp	Yes	
snmp-trap	162	a notification to the manager by SNMP of some event of interest	Yes	
StreamWorks	1558	a protocol for the transmission of high quality video (Xing)	Yes	
syslog	514	a protocol that allows a computer to send logs to other computer	Yes	
TACACS	49	an authentication protocol	Yes	
TFTP	69	Trivial File Transfer Protocol — a small, simple file transfer protocol used primarily in booting diskless systems	Yes	

## UDP Services

TABLE 16-2 UDP Services (continued)

Service Name	normal port number	Description	pre-defined in FireWall-1	Comments
time	37	a service that returns the time of day as a binary number	Yes	This is also a TCP service.
traceroute	>33000	a TCP/IP debugging application that shows the route followed by IP packets	Yes	
who	513	a service that provides information on who is logged on to the local network	Yes	

## RPC Services

TABLE 16-3 RPC Services

Service Name	program number	Description	pre-defined in Firewall-1	Comments
DCE-RPC		a protocol similar to Sun RPC Portmapper	Yes	Experimental support for use with Microsoft Exchange.
lockmanager	100021	a protocol used for the transmission of lock requests	Yes	as <i>nlckmgr</i>
mountd	100005	a protocol used for the transmission of file mount requests	Yes	belongs to the NFS group
NFS		Network File System — a protocol that provides transparent file access over a network	Yes	a group that includes all the services that are required for NFS.
nfsprog	100003		Yes	belongs to the NFS group
NIS		Network Information System — a protocol that provides a network accessible system administration database, widely known as Yellow Pages	Yes	NIS is a group that includes all the services that are required for NIS.
nisplus	100300		Yes	
pcnfsd	150001		Yes	belongs to the NFS group
rstat	100001	a protocol used to obtain performance data from a remote kernel	Yes	
rwall	100008	a protocol used to write to all users in a network	Yes	
ypbind	100007		Yes	belongs to the NIS group
yppasswd	100009		Yes	belongs to the NIS group
ypserv	100004		Yes	belongs to the NIS group
ypupdated	100028		Yes	belongs to the NIS group
ypxfrd	100069		Yes	belongs to the NIS group

## ICMP Services

**ICMP Services**

TABLE 16-4 ICMP Services

Service Name	Description	pre-defined in FireWall-1	Comments
dest-unreach	an ICMP message indicating that the destination is unreachable	Yes	
source-quench	an ICMP message indicating that the system cannot process datagrams at the rate at which they are being received	Yes	
info-req	an obsolete ICMP message	Yes	
info-reply	an obsolete ICMP message	Yes	
mask-request	an ICMP message requesting a diskless system's subnet mask	Yes	
mask-reply	an ICMP message in reply to a mask-request message	Yes	
param-prblm	an ICMP message indicating invalid data in an earlier message	Yes	
ping: echo-request, echo-reply	The ping program tests whether another host is available, and measures the time between the request (echo-request) and the reply (echo-reply).	Yes	
redirect	an ICMP error message sent by a router in response to a misdirected datagram	Yes	
time-exceeded	an ICMP error message indicating routing loops or reassembly failure	Yes	
timestamp (request, reply)	ICMP messages (request and reply) enabling systems to query each other for the current time	Yes	

## Other IP Protocol Services

TABLE 16-5 Other IP Protocol Services

Service Name	IP protocol number	Description	pre-defined in Firewall-1	Comments
egp	8	a protocol used to implement dynamic routing	Yes	
ggp	3	a protocol used to implement dynamic routing	Yes	
igrp	9	a protocol used to implement dynamic routing	Yes	
ospf	89	a protocol used to implement dynamic routing	Yes	

Other IP Protocol Services

400 FireWall-1 Architecture and Administration • September 1998

CHAPTER **17**

# FireWall-1 – Windows Interaction

## In This Chapter

<i>Registry</i>	<i>page 401</i>
<i>Windows NT Performance Monitoring</i>	<i>page 405</i>
<i>Windows NT Event Viewer</i>	<i>page 407</i>

## Registry

FireWall-1 modifies the Windows Registry under HKEY\_LOCAL\_MACHINE as follows:

### SOFTWARE\CheckPoint\

#### FireWall-1 GUI

These values relate to the FireWall-1 Windows GUI.

**TABLE 17-1** SOFTWARE\CheckPoint\FireWall-1 GUI

Value Name	Value Data
Vendor	The value determines the GUI icon.
Version	The FireWall-1 version



## Registry

## FireWall-1 GUI\4.0

TABLE 17-2 FireWall GUI\4.0

Value Name	Value Data
Build	Build number

## FW1

These values relate to the Management Server and the FireWall Module.

TABLE 17-3 SOFTWARE\CheckPoint\FW1

Value Name	Value Data
AddSnmp	flag indicating whether the connection was made to NT SNMP. If NT SNMP is not installed, FireWall-1 adds an SNMP extension. <ul style="list-style-type: none"> <li>■ 0x0 — Connection made to NT SNMP</li> <li>■ 0x1 — FireWall-1 SNMP extension was added</li> </ul>
Encryption	flag indicating whether encryption is installed <ul style="list-style-type: none"> <li>■ 0x0 — non VPN</li> <li>■ 0x1 — VPN</li> </ul>
FireWall	flag indicating whether FireWall Module is installed
FWDIR	directory under which FireWall-1 software is installed
Management	flag indicating whether Management Server is installed
ProductName	product number of installed product (for example, CPTW-IGW-1)
Unlimit	flag indicating whether unlimited gateway is installed (used by configuration application)

## FW1\CurrentVersion

There are no values under this key.

## FW1\SnmpAgent

This value serves to make the connection between NT SNMP and the FireWall-1 SNMP agent.

TABLE 17-4 SOFTWARE\FW1\SnmpAgent

Value Name	Value Data
Pathname	FireWall-1 SNMP DLL

**SYSTEM\****CurrentControlSet\Services\FW1****TABLE 17-5** SYSTEM\CurrentControlSet\Services\FW1

Value Name	Value Data
DependOnService	standard NT service attribute (not modifiable)
DisplayName	"FireWall-1"
Error Control	NT value
Group	"NDISWAN"
ImagePath	location of binary
LoadMode	indicates which stage of the two stage process is taking place
Start	0x2 - automatic
Type	0x1 - kernel driver

**CurrentControlSet\Services\FW1\Linkage****TABLE 17-6** SYSTEM\CurrentControlSet\Services\FW1\Linkage

Value Name	Value Data
Bind	device below to which FireWall-1 is bound
Export	name under which FireWall-1 is exported above
Route	NT value - set automatically during boot

**CurrentControlSet\Services\FW1\Parameters****TABLE 17-7** SYSTEM\CurrentControlSet\Services\FW1\Parameters

Value Name	Value Data
Debug	debug level
IPForwarding	flag indicated whether
License	license string
NewRAS	0x1 - indicates Microsoft Remote Access Service was installed after FireWall-1 installation

## Registry

## CurrentControlSet\Services\FW1\Performance

TABLE 17-8 SYSTEM\CurrentControlSet\Services\FW1\Performance values

Value Name	Value Data
Library	DLL containing functions for Close, Collect and Open values
Close	function (in Library DLL above)
Connect	function (in Library DLL above)
Open	function (in Library DLL above)
FirstCounter	Performance Monitor data
FirstHelp	Performance Monitor data
LastCounter	Performance Monitor data
LastHelp	Performance Monitor data

## CurrentControlSet\Services\FW0 (for NT 4.0 only)

Under NT 4.0, the FireWall-1 driver is loaded in a two-stage process, as follows:

TABLE 17-9 FireWall-1 driver - two stage loading process (NT 4.0)

Step	Module Loading
1	TCP
2	FWO (FireWall-1 first stage)
3	NDIS
4	NDISWAN
5	FW1 (FireWall-1 second stage)

The FWO values relate to the first stage.

TABLE 17-10 SYSTEM\CurrentControlSet\Services\FW0

Value Name	Value Data
DisplayName	"FireWall-1"
Error Control	NT value
Group	"PNP_TDI"
ImagePath	location of binary - another copy of the FW1 binary
LoadMode	indicates which stage of the two stage process is taking place
Start	<ul style="list-style-type: none"> <li>■ Ox02 — automatic startup</li> <li>■ Ox03 — manual startup</li> <li>■ Ox04 — startup disabled</li> </ul>
Type	Ox1 - kernel driver

## CurrentControlSet\Services\FW1SVC

TABLE 17-11 SYSTEM\CurrentControlSet\Services\FW1SVC

Value Name	Value Data
DisplayName	"Check Point FireWall-1 daemon"
Error Control	NT value
Group	"NDIS"
ImagePath	location of binary - another copy of the FW1 binary
ObjectName	NT attribute
Start	<ul style="list-style-type: none"> <li>■ 0x02 — automatic startup</li> <li>■ 0x03 — manual startup</li> <li>■ 0x04 — startup disabled</li> </ul>
Type	0x1 - kernel driver

## CurrentControlSet\Services\FW1SVC\Security

There are no FireWall-1 values under this key.

## CurrentControlSet\Services\FW1-&lt;NIC&gt;\Parameters\Tcpip

These values are copied from the real NIC at boot time.

## Windows NT Performance Monitoring

FireWall-1 provides performance statistics for the Windows NT Performance Monitor.

To view FireWall-1 statistics, proceed as follows:

## Windows NT Performance Monitoring

- 1 Open the Performance Monitor (in the Administrative Tools group).

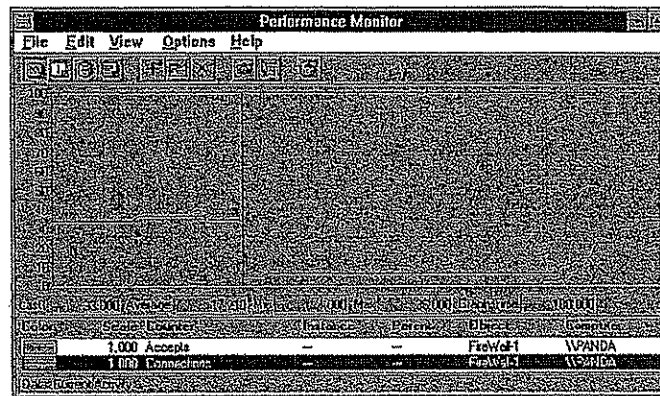


FIGURE 17-1 Performance Monitor window

- 2 Select the Add Counter button (  ) in the toolbar.

The Add to Chart window (FIGURE 17-2) is displayed.

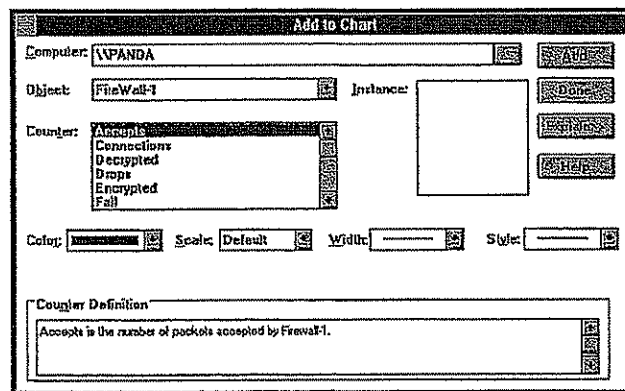


FIGURE 17-2 Add to Chart window

- 3 In the Add to Chart window, select FireWall-1 under Object.  
The Counters listbox shows all the FireWall-1 counters available.
- 4 Choose a counter you wish to monitor and click on Add.  
You may choose as many counters as you like.

5 If you wish to see an definition of each counter (under **Counter Definition** at the bottom of the window), click on **Explain**.

6 Select **Done** to close the **Add to Chart** window.

The Performance Monitor window then shows the FireWall-1 statistics (see FIGURE 17-1). For the most part, these are the same statistics that are available in the FireWall-1 System Status View.

## Windows NT Event Viewer

FireWall-1 posts System and Application (but not Security) events to the Windows NT Event Log. You can use the Windows NT Event Viewer application to view the Event Log.

FireWall-1 events are those whose Source is one of the following:

- FW1
- FireWall-1
- FW1SVC

Windows NT Event Viewer

408 FireWall-1 Architecture and Administration • September 1998



APPENDIX A

# Glossary

---

## A

**Access Control List  
(ACL)**

A sequential list of permit and deny conditions that define the connections permitted to pass through a device, usually a \*router. ACL syntax is arcane and specific to individual vendors, and a \*security policy based on ACLs is difficult to maintain.

**ActiveX**

A programming environment developed by Microsoft Corporation; a direct competitor to Sun Microsystems' \*Java. ActiveX presents a security risk because its executable ActiveX control files run on the client and can be used to gain illicit access to its files.

**ActiveX Stripping**

The ability to prevent \*ActiveX programs from being executed on the client by removing all ActiveX programs from HTML pages as they are downloaded.

**Address Resolution  
Protocol (ARP)**

The \*protocol used inside networks to bind high level \*IP addresses to low-level physical hardware addresses.

**anti-spoofing**

A method used to protect a network against \*IP spoofing attacks by verifying that a packet's source and destination \*IP addresses are appropriate to the interface through which the packet passes, for example, that a packet entering the local network from the outside carries an external source IP address.

A simple precaution against IP spoofing attacks is to hide internal IP addresses so that outside users cannot learn what they are.

409

anti-virus	A mechanism that provides detection, inoculation, logging and alerting capabilities to disarm *viruses on a local disk or in files as they are transferred on the network.
API	see "Application Programming Interface (API)"
application gateway	A *firewall that uses *proxies to provide security.  Historically, application level gateways suited the Internet's common uses and needs. However, as the Internet has become a dynamic environment in which new protocols, services and applications appear almost daily, proxies are no longer able to cope with the diversity of the Internet, or to fulfill the new business needs, high bandwidth and security requirements of networks.
application layer	The top network communication layer in a *protocol stack. The application layer is concerned with the semantics of work, such as how to format an e-mail message for display on the screen. A message's routing information is processed by lower layers of the network stack (see "layered communication model").
Application Programming Interface (API)	A well-defined set of functions, syntax or languages that enable application programs to communicate with one another and exchange data.
ARP	see "Address Resolution Protocol (ARP)"
Asynchronous Transfer Mode (ATM)	A method for dynamically allocating bandwidth using a fixed packet size (called a cell). These cells can carry data, voice, and video at high speeds.
ATM	see "Asynchronous Transfer Mode (ATM)"
audit	In network security, examining and evaluating the relative security of a network.

**authentication**

A method of verifying that an object is really what it appears to be: that a user or a computer is not being impersonated by another user or computer, or that a message received is the same message that was sent (that is has not been tampered with).

Users are authenticated by a challenge-response mechanism: the user is asked to provide information (for example, a \*password or \*token) presumably known to no one else. Computers may be authenticated in a similar way. In addition, human users can be authenticated by biometric means, such as verifying fingerprints or retinal images.

Authenticating a message verifies its integrity, usually by means of a \*digital signature.

**authentication  
algorithm**

An algorithm, such as MD5, used to calculate the \*digital signature by which a message's integrity is verified.

**B****B1, B2 level**

In the U.S., the National Security Agency's rating system for network security. Ratings are certified by the National Computer Security Center. A B1 rating describes a basic level of enterprise-wide Internet security and is equivalent to the European E3 rating (*see* "E3"). A B2 rating describes a much higher level of security typically used to protect military systems.

**bridge**

A device, with two interfaces connecting two networks, that replicates packets appearing on one interface and transmits them on the other interface.

**broadcast**

A message sent to every destination on the network, in contrast to \*multicast and \*unicast.

**C****certificate**

A \*digital signature encrypted with the (for example, \*RSA) private key of the \*Certificate Authority (CA) who sent the message that includes the certificate, intended to generate confidence in the legitimacy of the public key contained in the message.

The recipient can verify that the message was indeed sent by the CA by computing the message's digital signature, decrypting the transmitted digital signature using the CA's public key (reliably available from an out-of-band

source such as a printed directory) and comparing the two. If they are the same, then the message was sent by someone who knows the CA's private key; presumably this can only be the CA.<sup>1</sup>

**Certificate Authority  
(CA)**

A trusted third party from which information (for example, a person's public key) can be reliably obtained, even over an insecure channel.

For example, if Alice and Bob obtain each other's public keys over an insecure channel such as the Internet, they must be certain that the keys are genuine. Alice cannot simply ask Bob for his public key, because there is the danger that Charlie might intercept Alice's request and send Alice his own key instead. Charlie would then be able to read all of Alice's encrypted messages to Bob.

The CA certifies the information it provides by generating a \*certificate. Anyone receiving the information verifies the certificate as proof of the information's validity.

**community**

In SNMP, a community is a logical group of managed devices and NMSs in the same administrative domain.

**computationally  
unfeasible**

Impossible in practical terms though not theoretically so. For example, it is computationally unfeasible to compute the private part of a \*public key pair from the public part, because the only known method — the "brute force" approach of trying all the possibilities one after the other — would take millions of years.

**connectionless  
communication**

A scheme in which communication occurs outside of any context, that is, replies and requests are not distinguishable. Connectionless communication avoids the overhead inherent in maintaining a connection's context, but at the risk of allowing transmission errors to go undetected. Streaming services usually use connectionless communication protocols such as \*UDP, because they must attain high transmission speeds and there is no advantage in sending a retransmitted packet out of sequence.

1. Purists would object to saying "encrypted with the private key" and "decrypted with the public key." The words "encrypted" and "decrypted" are used here in their common senses of hiding and revealing.

content security

The ability to specify the content of a communication as an element of a security policy, in contrast to defining a security policy on the basis of header information only. Effective content security requires that a firewall understand the internal details of the protocols and services it monitors.

An example of content security is enforcing \*anti-virus checking for downloaded files, disallowing emails from or to specified email addresses, or allowing access to Web pages containing certain words only during specified time periods.

Content Vectoring  
Protocol (CVP)

An \*OPSEC API that enables integration of third-party content security applications such as anti-virus software into FireWall-1. The CVP API has been adopted by a wide variety of security vendors.

## D

Data Encryption  
Standard (DES)

An widely-used \*secret key \*encryption algorithm endorsed as an official standard by the U.S. government in 1977. To address security concerns resulting from the relatively short (56 bit) key length, triple-DES (encrypting under three different DES keys in succession, believed to be equivalent to doubling the DES key length to 112 bits) is often employed.

data link layer (DLL)

see "layered communication model"

### Demilitarized Zone (DMZ)

A computer or a network located outside the trusted or secure network but still protected from the unsecure network (Internet). Network administrators often isolate public resources such as HTTP servers in a DMZ so that an intruder who succeeds in breaching security cannot continue on to the internal network.

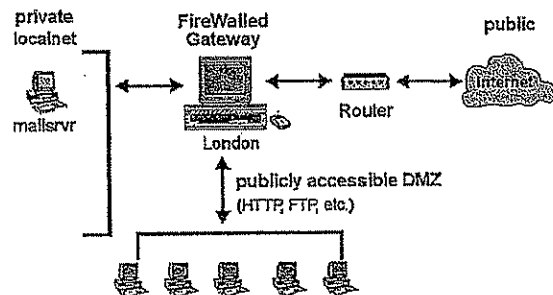


FIGURE A-1 A network with a Demilitarized Zone

In FIGURE A-1, the DMZ is protected by the FireWalled gateway but is at the same time isolated from the private network. There is no way of connecting from the DMZ to the private network without going through the \*firewall.

### denial of service attack

An attack with the purpose of overwhelming the target with spurious data to the point where it is no longer able to respond to legitimate service requests, in contrast to an attack whose purpose is to penetrate the target system. Examples of denial of service attacks are SYN and "ping of death."

### dial-up line

A telecommunication line available only after a dialling procedure, such as an ordinary telephone line, in contrast to a \*leased line.

### Diffie-Hellman key exchange scheme

A public key scheme, invented by Whitfield Diffie and Martin Hellman, used for sharing a secret key without communicating any secret information, thus avoiding the need for a secure channel. Once the correspondents have computed the shared secret key, they can use it to encrypt communications between them.

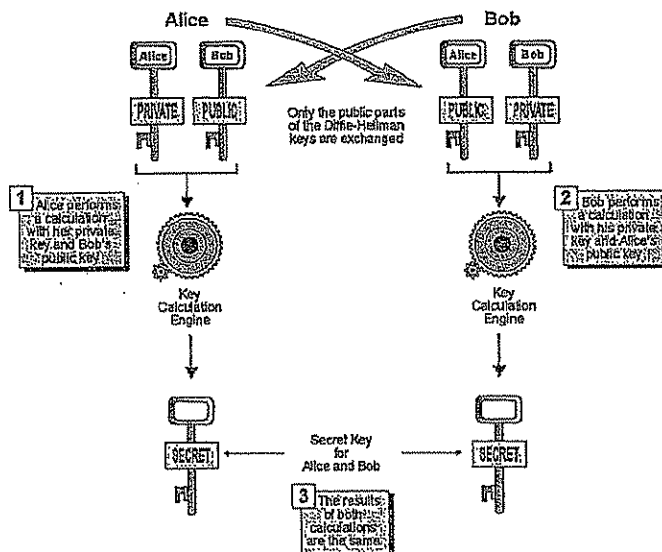


FIGURE A-2 Diffie-Hellman Key Exchange

Under the Diffie-Hellman scheme, each correspondent has a public-private key pair. They agree on a secret key as follows (FIGURE A-2):

- Bob gets Alice's public key (from a \*Certificate Authority) and performs a calculation involving his own private key and Alice's public key.
- Alice gets Bob's public key (from a Certificate Authority) and performs a calculation involving her own private key and Bob's public key

The results of both calculations are the same, and serves as the secret key. In this way, a secret key can be agreed on without any secret information being communicated. There is no opportunity for an eavesdropper to determine the secret key.

An additional advantage of this scheme is that only one key pair needs to be managed for each correspondent.

#### digital signature

The result of a complex calculation on the contents of a message. Changing even one bit in the message results in a completely different digital signature. Moreover, it is \*computationally unfeasible to compose a message:



with a given digital signature. A digital signature is used to verify a message's integrity, that is, to ensure that it has not been tampered with. *See also* certificate.

#### directory service

A standard database providing distributed, scalable, client/server-based repositories of data that are read much more frequently than modified (for example, user definitions, user profiles, and network resource definitions). Users and applications can access these directories through directory access protocols (DAPs). In network environments, example DAPs include the Novell Directory Services (NDS) and \*X.500 directory access protocols. Another widely-used DAP is LDAP (*see* "Lightweight Directory Access Protocol (LDAP)").

#### DMZ

*see* "Demilitarized Zone (DMZ)"

## E

#### E3

A verifiable level of security required by European governments for any Internet firewalls employed over any of its networks. Products meeting this level of security (roughly equivalent to the U.S. B1 "Orange Book" level) are certified by the Information Technology Security Evaluation and Certification organization (ITSEC) in the United Kingdom and by the Logica Evaluation Defence Signals Directorate (DSD) in Australia. *See also* "B1, B2 level".

"E3" also refers to a high speed transmission line in Europe equivalent to the T3 transmission line in the United States.

#### encapsulated encryption

An \*encryption scheme in which an entire packet, including the header, is encrypted, and a new header appended to the packet. Encapsulated encryption hides the true source and destination but increases a packet's length, in contrast to \*in-place encryption.

#### encryption

The transformation of a message so that the encrypted message can only be read with the aid of some additional information (the \*key) known to the sender and the intended recipient alone.

In \*secret key (symmetric) encryption, the same key is used to both encrypt a message and then to decrypt it. In \*public key (asymmetric) encryption, two mathematically-related keys are used: one to encrypt the message and the other to decrypt it.

#### encryption algorithm

An algorithm, such as \*DES, for encrypting and decrypting data. An encryption algorithm is one element of an \*encryption scheme.

**encryption domain**

The computers and networks on whose behalf a \*gateway encrypts and decrypts communications.

**encryption scheme**

A mechanism for encrypting and authenticating messages as well as managing and distributing keys, such as \*FWZ, \*IPsec, \*SKIP and \*ISAKMP. An encryption scheme consists of three elements:

- an \*encryption algorithm that performs the actual encryption
- an \*authentication algorithm for ensuring message integrity
- a \*key management protocol for generating and exchanging keys

**enterprise-wide  
security management**

The consistent application and management of a security policy in a complex, distributed network environment, usually including corporate \*intranets and \*extranets.

**extranet**

In contrast to the Internet, which provides universal access to network-based information, and an \*intranet, which is accessible only within an enterprise, an extranet enables a company and its partners or customers to collaborate, communicate and exchange documents in a secured network environment. extranets typically utilize virtual private networks that allow authorized users to access specific information, such as technical documentation or inventory information (see "Virtual Private Network (VPN)").

**F****File Transfer Protocol  
(FTP)**

A widely-used TCP-based protocol for copying files between hosts. In security environments, FTP commands can be controlled via \*authentication schemes, \*content security schemes, file name restrictions, and \*anti-virus programs.

**firewall**

A combination of hardware and software resources positioned between the local (trusted) network and the Internet (see FIGURE A-3). The firewall ensures that all communication between an organization's network and the

Internet conform to the organization's security policy. Firewalls track and control communications, deciding whether to pass, reject, encrypt or log communications.

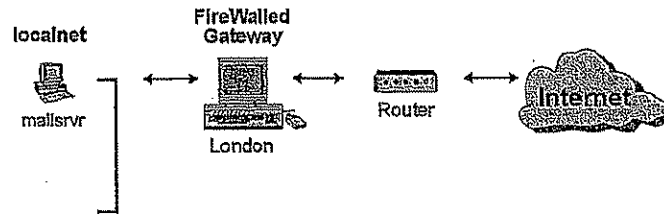


FIGURE A-3 A network protected by a firewalled gateway

#### FireWall Module

A FireWall-1 security application, similar to an \*Inspection Module, that provides the additional functionality of \*user authentication, \*content security, \*encryption, \*Network Address Translation, and \*high availability.

#### Fortezza

A family of security algorithms that ensure data integrity (Secure Hash Algorithm), authentication, non-repudiation (Digital Signature Algorithm), and confidentiality (Key Exchange Algorithm and Skipjack Algorithm). "Fortezza-enabled" and "Fortezza Certified" are terms applied to commercial hardware and software products that use one or more of these Fortezza security algorithms.

#### frame

The packet transmitted by the \*data link layer.

#### FTP

see "File Transfer Protocol (FTP)"

#### FWDIR

An environment variable specifying the directory in which FireWall-1 is installed.

#### FWZ

Check Point's domestic and worldwide exportable \*encryption scheme, offering \*Diffie-Hellman key exchange, multiple \*encryption algorithms, \*authentication, and \*Certificate Authority capabilities.

## G

### gateway

A device positioned between two networks through which all communications between the networks must pass. A gateway is a natural choice for enforcing a security policy and providing encryption and authentication services.

### gateway stealthing

Disallowing connections that originate or terminate on a \*gateway while allowing connections to pass through the gateway, thereby making the gateway transparent (or "invisible") to the networks which it connects.

## H

### header

The portion of a packet, preceding the actual data, containing source and destination addresses, checksums and other fields. A header is analogous to the envelope of a letter sent by ordinary mail. In order to deliver the message (letter), it is only necessary to act on the information (address) in the header (envelope).

A communication can have several layers of headers. For example, a mail message includes an application layer header specifying, the message originator, date and time. At the lower layers, the packets in which the mail message is transmitted carry IP headers and TCP headers.

### high availability

A hardware and software configuration in which a device takes over the tasks of another device that has gone down.

### host

A computer connected to a network.

### HTTP

*see* "Hypertext Transfer Protocol (HTTP)"

### hub

A device that connects computers, servers and peripherals together in a local area network (LAN). Hubs typically repeat signals from one computer to the others on the \*LAN. Hubs may be passive or intelligent and can be stacked together to form a single managed environment. *See also* "switch" and "router".

### Hypertext Transfer Protocol (HTTP)

A standard protocol for transferring files on the World Wide Web.

# I

## IETF

*see* "Internet Engineering Task Force (IETF)"

## in-place encryption

A mechanism by which only the data in an IP packet is encrypted, while the header is not encrypted. In-place encryption leaves headers exposed, but preserves the packet's length, in contrast to \*encapsulated encryption.

## Information Technology Security Evaluation and Certification Scheme (ITSEC)

An organization dedicated to evaluating the security features of information technology products and systems and to certifying the level of assurance that can be placed on them.

## INSPECT

Check Point's high-level scripting language for expressing a \*Security Policy. An INSPECT script is compiled into machine code and loaded into an \*Inspection Module for execution.

## Inspection Code

Inspection Code compiled from an Inspection Script and loaded into a FireWall-1 FireWall Module for enforcement.

## Inspection Module

A FireWall-1 security application embedded in the operating system kernel, between the data link and network layers, that enforces a FireWall-1 \*Security Policy. *See also* "FireWall Module".

## Inspection Script

The ASCII file generated from the \*Security Policy by FireWall-1 is known as an Inspection Script.

An Inspection Script can also be written using a text editor.

## Internet

A public network connecting many thousands of computer networks in a three-level hierarchy including backbone networks (for example, NSFNET, MILNET), mid-level networks and stub networks. The Internet utilizes multiple communication protocols (especially TCP/IP) to create a worldwide communications medium.

## Internet Engineering Task Force (IETF)

The principle body engaged in the development of new Internet standard specifications. IETF identifies solutions to technical problems and makes recommendations to the Internet Engineering Steering Group (IESG)

regarding the standardization of protocols and protocol usage in the Internet, and facilitates the transfer of technology developed by the Internet Research Task Force (IRTF) to the wider Internet community. IETF also provides a forum for the exchange of information between vendors, users and researchers interested in improving various aspects of the Internet. The IETF meets three times a year and is comprised entirely of volunteers.

**Internet Protocol (IP)**

The network layer for the TCP/IP protocol suite. IP is a connectionless, best-effort packet switching protocol designed to provide the most efficient delivery of packets across the Internet.

**Internet Protocol  
Security Standard  
(IPSec)**

An encryption and authentication scheme supporting multiple encryption and authentication algorithms.

**Internet Security  
Association Key  
Management Protocol  
(ISAKMP)**

A standard protocol for authentication and key exchange; part of the key management scheme used for negotiating virtual private networks (VPNs) as defined in the IETF IPSec working group. This key management scheme is mandated for deployment in IPv6.

**Internet Service  
Provider (ISP)**

A provider of access to the Internet. In some cases, these providers own the network infrastructure, while other lease network capacity from a third party.

**intranet**

An internal private network, managed according to Internet protocols, but accessible only inside the organization.

**IP**

*see* "Internet Protocol (IP)"

**IPSec**

*see* "Internet Protocol Security Standard (IPSec)"

**IP address**

The 32-bit address defined by the Internet Protocol to uniquely identify Internet hosts and servers. A typical IP Address, shown here in conventional IP "dot" notation, consists of the following parts:

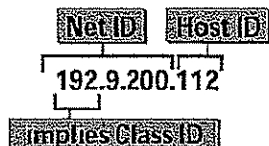


FIGURE A-4 IP Address

The first bits of the Class ID specify a network's class. Most local networks are of class C (Class ID byte = 110XXXXX; Class ID  $\geq 192$  in IP dot notation). Class C networks can have up to 254 hosts. Larger networks can be either class B or Class A.

The Net ID identifies the network. Because an IP address consists of both a network identifier (NetID) and a host identifier (HostID), it does not identify a host, but rather a network connection (interface). If a host or gateway is connected to several networks, it will have several IP addresses.

By convention, host ID 0 refers to the network itself; that is, a network's address ends in zeros. This scheme enables IP addresses to specify networks as well as hosts. A host identifier of all 1s is reserved for broadcast.

**IP spoofing**

A technique whereby an intruder attempts to gain access by altering a packet's IP address to make it appear as though the packet originated in a part of the network with higher access privileges (for example, the IP address of a workstation in the local network). This form of attack is only possible if a network's internal IP addresses have been exposed (*see* "anti-spoofing").

**ISP**

*see* "Internet Service Provider (ISP)"

**ISAKMP**

*see* "Internet Security Association Key Management Protocol (ISAKMP)"

**ITSEC**

*see* "Information Technology Security Evaluation and Certification Scheme (ITSEC)"



## J

### Java

A platform-independent programming environment developed by Sun Microsystems and supported by numerous vendors, including Microsoft. Java presents a security risk because Java applets run on the client and can be used to gain illicit access to its files.

### Java Stripping

The ability to prevent \*Java code from being executed on the client by removing all Java tags from HTML pages as they are downloaded.

## K

### Kerberos

An authentication service developed by the Project Athena team at MIT. Kerberos uses secret keys for encryption and authentication. Unlike a public key authentication system, it does not produce digital signatures; Kerberos was designed to authenticate requests for network resources rather than to authenticate authorship of documents. Thus, Kerberos does not provide for third-party verification of documents.

### key

Information used to encrypt and decrypt data. There are two kinds of keys: \*secret keys and \*public keys.

### key management

A mechanism for distributing encryption keys in a public key scheme. Key management is performed by a \*Management Station and includes key generation, certification (although this can also be performed by an external \*Certificate Authority) and key distribution. Key management can either be manual or automated.

## L

### LAN

*see* "Local Area Network (LAN)"

### layered communication model

The conceptual division of communication tasks into a "layered model." The fundamental characteristic of the layered model is that each layer processes the same object processed by the corresponding layer at the other end of the communication.

The X.25 protocols shown in FIGURE A-5 are based on the OSI model.

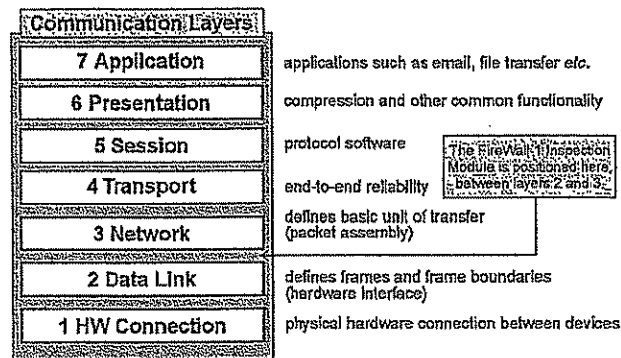


FIGURE A-5 OSI seven layer communication model

The TCP/IP model, consisting of four software layers and one hardware layer, is illustrated in FIGURE A-6.

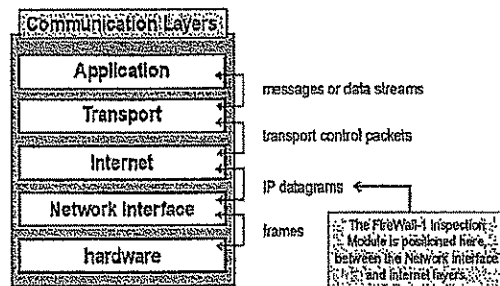


FIGURE A-6 TCP/IP communication model

### leased line

A dedicated telecommunications access line that is "leased" from a vendor, and thus always available, in contrast to a \*dial-up line. The physical medium may be copper or fiber optic, providing a wide range of line speeds.

**Lightweight Directory  
Access Protocol (LDAP)**

A mechanism for Internet clients to access and manage a database of directory services over a TCP/IP connection. A simplification of the X.500 directory access protocol, LDAP is gaining significant support from major Internet vendors.

**load balancing**

The ability to distribute processing loads among multiple servers to improve performance and reduce access times. Load balancing is often transparent to the user and improves Internet security by reducing the risks associated with certain attacks and by applying greater resources to the task of monitoring and filtering network traffic. A variety of algorithms may be used to determine how best to distribute traffic over these servers.

**Local Area Network  
(LAN)**

A data network intended to serve an area of only a few square kilometers or less (more typically, an individual organization). LANs consist of software and equipment such as cabling, hubs, switches and routers, enabling communication between computers and the sharing of local resources such as printers, databases, and file and video servers.

**Logging and Event API  
(LEA)**

An \*OPSEC API that enables an application to securely receive and process both real-time and historical logging and auditing events generated by FireWall-1. LEA can be used by a variety of applications to complement firewall management.

**M****MAC address**

The physical hardware address of a device connected to a network.

**Managed Internet  
Security Services**

Bundled security services, including secure \*Internet, \*intranet and \*extranet, provided by an \*ISP. Typically, the ISP handles management and support for the security services, which can be implemented as part of the Internet service implementation or customized to client needs.

**Management Module**

The FireWall-1 module in which a FireWall-1 \*Security Policy is defined. *See also* "Management Station".

**Management Server**

The FireWall-1 application, controlled by a GUI on a client, that manages a FireWall-1 \*Security Policy. *See also* "Management Station".

**Management Station**

The workstation on which a FireWall-1 \*Management Module runs. If the Management Module is deployed in Client/Server mode, then the Graphical User Interface (GUI) can be run on another workstation, while the Management Station runs the \*Management Server that supports the GUI.

**Manual IPsec**

*see* "IPSec".

**Master**

In FireWall-1, the station to which logs and alerts are directed.

The Master also maintains the most recent Inspection Code for each of the FireWalled systems it controls. If a FireWalled system loses its Inspection Code for any reason, it can retrieve an up-to-date copy from the Master. In practice, the Master and Management Station are usually on the same system, but Failover Masters can be defined.

**multicast**

A message sent to all the destinations in a specific group of hosts in a network, in contrast to \*broadcast and \*unicast.

**multi-homed host**

A computer with two or more physical network connections is often referred to as a multi-homed host.

**N****NAT**

*see* "Network Address Translation"

**network address**

The network portion of an IP address. Depending on the class of network; this may comprise the first one to three bytes of an IP address, with the remainder being the host or server address.

**Network Address  
Translation**

Translating an internal network's real IP addresses to "false" IP addresses, either to prevent exposing the real addresses or to enable hosts with "invalid" addresses to communicate on the Internet, thus avoiding the need to change a network's IP addresses (a formidable, error-prone task).

**NIC**

Network Interface Card; also Network Information Center, an organization that provides services to Internet networks and users.

## O

Open Platform for  
Secure Enterprise  
Connectivity (OPSEC)

An open, industry-wide alliance, driven by Check Point Software Technologies, to ensure interoperability at the policy level between security products. Interoperability is achieved through a combination of published APIs, industry-standard protocols, and a high-level scripting language. OPSEC encourages partnerships in the areas of infrastructure (network products and services), framework (security products), and passport (applications developers).

## OPSEC

*see* "Open Platform for Secure Enterprise Connectivity (OPSEC)"

## P

## packet

A unit of data as sent across a network.

## packet filter

A type of \*firewall that examines only the network layer, typically implemented by \*routers. This type of firewall cannot support dynamic protocols and cannot apply application intelligence to the data stream.

## password

a short string of characters, knowledge of which is required to gain access to some resource. Passwords are considered unreliable security devices because they are relatively easy to guess at, and people tend not to take strict precautions against their disclosure. *See also* "token".

PPP (Point-to-Point  
Protocol)

A method for transmitting packets over serial point-to-point links, such as a \*dial-up line.

PPTP (Point-to-Point  
Tunneling Protocol)

An extension to PPP that encapsulates different protocols, including IPX and Appletalk, into an IP data stream so that they can be transmitted over the Internet.

## protocol

A formal description of message formats and the rules required to accomplish some task.

**protocol stack**

A synonym (in practice if not in theory) for the \*communication layers as supported by an operating system.

**proxy**

An application-layer implementation of a service that provides additional functionality (for example, security or caching) that is not part of the original service.

Application gateways use proxies to implement firewalls. A proxy's primary advantage is its ability to provide partial communication-derived state, full application-derived state information and partial communication information.

The disadvantages of using proxies as firewalls are:

- **limited connectivity** — each service needs its own proxy, so the number of available services and their scalability are limited, and there is usually a significant delay before a new service can be implemented (a new proxy must be written)
- **limited technology** — application gateways cannot provide proxies for UDP, RPC and other services from common protocol families
- **performance** — application level implementation entails a discernible performance penalty

In addition, proxies are vulnerable to OS and application level bugs, overlook information contained in lower layers, and in the case of traditional proxies, are rarely transparent.

**public key**

A scheme in which each correspondent has a pair of mathematically related keys: a public key known to everyone, and a private key known only to its owner.

- The \*RSA public key scheme is used for encryption as follows: if Bob wants to send Alice an encrypted message, he encrypts the message with Alice's public key. The encrypted message can only be decrypted with Alice's private key, which only Alice knows.
- The \*Diffie-Hellman public key scheme is used for sharing a secret key without communicating any secret information, thus avoiding the need for a secure channel.

The disadvantage of public key encryption is that it is much slower than \*secret key encryption.

The terminology can be confusing, because "public key" is sometimes used to mean both keys together (in the context of schemes) and sometimes to mean only the public part of the key.

**Public Key  
Infrastructure (PKI)**

A set of security services, usually provided by a \*Certificate Authority, enabling \*authentication, \*encryption and certificate management using \*public key encryption technology.

**public network**

Any computer network, such as the Internet, that offers long-distance inter-networking using open, publicly accessible telecommunications services, in contrast to a \*WAN or \*LAN.

## R

**RC2, RC4**

A widely used \*encryption method developed by Rivest Corporation for RSA Data Security.

**Remote Authentication  
Dial In Service  
(RADIUS)**

A centralized network-authentication scheme developed by Livingston Enterprises and proposed as a standard to the IETF, which includes \*authentication, authorization, and accounting features and may also include the ability to pass-through authentication to proxy servers.

**Request For Comments  
(RFC)**

A numbered series of documents, available from \*NIC, which are the primary means of technical discussion about the Internet. Some RFCs define standards.

**Resource Reservation  
Protocol (RSVP)**

A \*unicast and \*multicast signaling \*protocol, designed to install and maintain reservation state information at each router along the path of a stream of data. RSVP-enabled applications may improve the quality of service across IP networks. Networked multimedia applications, many of which benefit from a predictable end-to-end connection, are likely to be initial users of RSVP-signaled services.

**RFC**

see "Request For Comments (RFC)"



**router**

A device providing network-to-network transmission capabilities, including routing, segmenting and filtering. Most routers support multiple communications protocols, such as ISDN and Ethernet. By examining only packet headers, routers can:

- pass the packets between networks running different protocols
- determine which network should receive the packet
- determine whether to block the transmission

**Rule Base**

An ordered set of rules that defines a FireWall-1 \*Security Policy. A rule describes a communication in terms of its source, destination and service, and specifies whether the communication should be accepted or rejected, as well as whether it is to be logged. Each communication is tested against the Rule Base; if it does not match any of the rules, it is dropped.

**RSA**

A public key scheme used for \*encryption and \*digital signatures, invented in 1977 by Ron Rivest, Adi Shamir and Leonard Adelman; also a company founded by them to market products based on their inventions.

**S****SAM**

see "Suspicious Activity Monitoring Protocol (SAM)"

secret key

A key used to both encrypt and decrypt data.

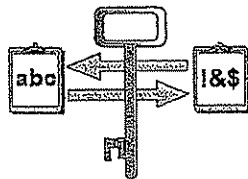


FIGURE A-7 Encrypting and decrypting with a secret key

Ensuring the key's secrecy is critical, since anyone who knows the key can decrypt and read the message.

Secret key encryption is simple and fast, but has some disadvantages:

- A secure channel is required by which the correspondents can agree on a key before their first encrypted communication.  
Direct face-to-face negotiation may be impractical or unfeasible, and the correspondents may have to agree on a key by mail or telephone or some other insecure means.
- The number of keys required can quickly become unmanageable, since there must be a different key for each pair of possible correspondents.

Public (asymmetric) key systems, where each correspondent has a pair of keys, can solve both of these problems (*see* "public key").

#### Secure Hypertext Transfer Protocol (S-HTTP)

A security-enhanced version of \*HTTP providing a variety of mechanisms to enable confidentiality, \*authentication and integrity. Unlike SSL, which layers security beneath application protocols like HTTP, NNTP, and Telnet, S-HTTP adds message-based security to HTTP. SSL and S-HTTP can co-exist by layering S-HTTP on top of SSL.

#### Secure Socket Layer (SSL)

A protocol combining \*RSA \*public key encryption and the services of a \*Certificate Authority to provide a secure environment for electronic commerce and communications. SSL provides three levels of security server authentication:

- verification of the identity of the server using a \*certificate
- \*encryption, which ensures the privacy of client-server communications by encrypting the data stream

- integrity, which verifies that the contents of the message arrive at their destination in the same form as they were sent.

#### Security Policy

A Security Policy is defined in terms of firewalls, services, users, and the rules that govern the interactions between them. Once these have been specified, an \*Inspection Script is generated and then installed on the firewalled hosts or gateways. These gateways can enforce the Security Policy on a per-user basis, enabling verification not only of the communication's source, destination and service, but the authenticity of the user as well. A user-based Security Policy also allows control based on content. For example, mail to or from certain addresses can be rejected or redirected, access can be denied to specific URLs, and anti-virus checking of transferred files can be performed.

#### S-HTTP

see "Secure Hypertext Transfer Protocol (S-HTTP)"

#### Simple Key Management for Internet Protocols (SKIP)

An automated \*key management system developed by Sun Microsystems and proposed to the IETF as a standard \*IPSec key management scheme. SKIP adds key management functionality to IPSec. Several vendors have successful implementations of SKIP, and both SKIP and \*ISAKMP can be deployed/implemented within the IPSec framework.

#### Simple Mail Transfer Protocol (SMTP)

A \*protocol used to transfer electronic mail between computers. Subsequently enhanced to support not only e-mails but file attachments as well, SMTP's flexibility poses a challenge to security systems.

#### Simple Network Management Protocol (SNMP)

A \*protocol for managing nodes on an IP network. In security environments, SNMP is used to communicate management information (monitoring, configuration and control) between the network management stations and network elements (for example, devices such as hosts, gateways and servers).

#### SKIP

see "Simple Key Management for Internet Protocols (SKIP)"

#### SMTP

see "Simple Mail Transfer Protocol (SMTP)"

#### SNMP

see "Simple Network Management Protocol (SNMP)"

SSL

see "Secure Socket Layer (SSL)"

#### state information

Information describing the context of a communication. There are two types of state information: communication derived and application derived.

- Communication-derived state information is extracted from past communications and is compared against current attempts to access or manipulate information. For example, an outgoing PORT command of an \*FTP session can be saved so that a later incoming FTP data connection can be verified against it.
- Application-derived state information is extracted from other applications to verify user access. For example, an \*extranet application may be used to allow a previously authenticated access through the firewall for authorized services only.

#### Stateful Inspection

A technology developed and patented by Check Point that provides the highest level of security currently available. A stateful \*Inspection Module accesses and analyzes all the data derived from all communication layers. This state and context data is stored and updated dynamically, providing virtual session information for tracking connectionless protocols.

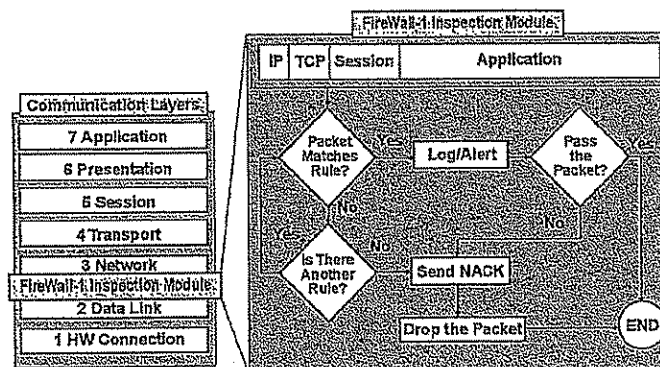


FIGURE A-8 Stateful Inspection

Cumulative data from the communication and application states, network configuration and security rules are all used to decide on an appropriate action, either accepting, rejecting or encrypting the communication (FIGURE A-8).

Any traffic not explicitly allowed by the \*Security Policy is dropped.

TABLE A-1 Technology Comparison

firewall capability	routers	proxies	Stateful Inspection
communication information	Partial	Partial	Yes
communication-derived state	No	Partial	Yes
application-derived state	No	Yes	Yes
information manipulation	Partial	Yes	Yes

#### stub network

A network that carries only packets to and from local hosts. Even if it has paths to more than one network, a stub network does not carry traffic for other networks. Stub networks are the third and last layer of the Internet network topography.

#### subnet

A physically independent network segment, which shares a network address with other portions of the network. Subnets enable greater security from unauthorized internal access by dividing the intranet into discrete managed portions.

#### Suspicious Activity Monitoring Protocol (SAM)

An \*OPSEC API used to integrate third party intrusion detection applications into firewalls.

#### switch

A hub-like device that maximizes the performance of a high-speed connection by providing a dedicated link between two devices via MAC-layer addresses.

#### symmetric key

see "secret key"

## T

#### TELNET (Telecommunications Network Protocol)

A remote terminal protocol enabling any terminal to login to another host.

#### TCP

see "Transmission Control Protocol"

**TCP/IP**

*see* "Transmission Control Protocol over Internet Protocol (TCP/IP)"

**token**

A \*password that can be used only once, typically generated as needed by a hardware device. Tokens are considered to be secure because even if one is revealed, it cannot be misused because it is no longer valid after its first use.

**Transmission Control Protocol**

An connection-oriented and stream-oriented Internet standard transport layer protocol, in contrast to the connectionless UDP protocol ("User Datagram Protocol (UDP)").

**Transmission Control Protocol over Internet Protocol (TCP/IP)**

The common name for the suite of UNIX-based protocols developed by the U.S. Department of Defense in the 1970s. TCP/IP is the primary language of the Internet.

**U****UDP**

*see* "User Datagram Protocol (UDP)"

**unicast**

A message sent to a single destination, in contrast to \*broadcast and \*multicast.

**Uniform Resource Locator (URL)**

An address format used by Internet communications protocols such as the \*Hyper Text Transfer Protocol (HTTP) popularized by the World Wide Web. URLs typically identify the type of service required to access an item, its location on an Internet host and the file name or item name on that machine.

**URL**

*see* "Uniform Resource Locator (URL)"

**URL Filtering Protocol (UFP)**

An \*OPSEC API that enables the integration of third-party application to categorize and control access to specific URL addresses.

**user authentication**

The process of verifying that a user is actually who he or she claims to be. *See also* "authentication".

User Datagram  
Protocol (UDP)

An Internet-standard transport layer protocol which adds a level of reliability and multiplexing to IP. UDP is a connectionless protocol, making no distinction between the originator of the request and the response to it. Connectionless protocols are problematic in a security environment, but can be tracked and controlled using communication-derived state information (*see* "state information").

## V

Virtual Private Network  
(VPN)

A network with some public segments in which data passing over its public segments is encrypted to achieve secure communications. A VPN is significantly less expensive and more flexible than a dedicated private network.

virus

A program that replicates itself on computer systems by incorporating itself into other programs which are shared among computer systems. Once in the new host, a virus may damage data in the host's memory, display unwanted messages, crash the host or, in some cases, simply lie dormant until a specified event occurs (for example, the turning of a new year).

VPN

*see* "Virtual Private Network (VPN)"

## W

WAN

*see* "Wide Area Network (WAN)"

Web Server

A network device that stores and serves up any kind of data file, including text, graphic images, video, or audio. Its stored information can be accessed via the Internet using standard protocols, most often \*HTTP.

Wide Area Network  
(WAN)

A (usually private) geographically large network. A WAN is typically constructed to span numerous locations within a single city.



World Wide Web  
(WWW)

A hypertext-based information service providing access to multimedia, complex documents and databases via the Internet. Web application programs can access many other Internet services as well, including Gopher, Usenet news, file transfer, remote connectivity and even special access to data on the local network.

WWW

*see* "World Wide Web (WWW)"

X

X.25

A widely-used set of \*protocols based on the OSI model. *See also* "layered communication model".

X.500

A \*protocol used for communication between a user and an X.500 directory services system. Multiple X.500 directory system agents may be responsible for the directory information for a single organization or organizational unit.

X.509

A certification methodology providing authenticated, encrypted access to private information, which establishes a trust model enabling certain transactions such as those involving money or funds. For example, X.509 certificates are used in the \*ISAKMP encryption scheme to obtain public keys and to verify the authenticity of the parties in an exchange.

438 FireWall-1 Architecture and Administration • September 1998

# Master Index

## SYMBOLS

#define  
     difference between #define and define, AA-302,  
     AA-311  
 \$FWDIR/conf/smtp.conf  
     description, AA-111  
 \$FWDIR/conf/xdate.conf  
     explanation of fw\_x\_translation table, AA-215  
 \$FWDIR/log/fw.log, AA-265  
 .EPF files, VP-122

## NUMERICS

3Com routers  
     managing in the rule base, WI-47, OL-46  
     setup, WI-42

## A

abandon parameter  
     smtp.conf, AA-111  
 Accept Domain Name Download, OL-111, OL-115  
 Accept Domain Name Queries, OL-111, OL-115  
 Accept ICMP, WI-145, OL-111, OL-116  
 Accept Outgoing Packets, OL-110  
 Accept Outgoing Packets property, WI-178  
 Accept RIP, OL-110, OL-115  
 Accept UDP Replies, OL-110  
 access

    limiting to specific ports, AA-355  
     restoring, to blocked system, AA-336  
 Access Control  
     logging, AA-225  
 Access Lists  
     managing imported access lists, OL-140  
     Properties, WI-148, OL-115  
     router, installing, WI-200, OL-142  
     router, uninstalling, OL-142  
     Wallfleet, AA-280  
 Account Management, AA-135, WI-94  
     defining users in both LDAP and  
     FireWall-1, AA-142, AA-154  
 Account Management Client, WI-74  
     installation error message, AM-10  
     installing, AM-8  
     JRE installation, AM-13  
     location on CD-ROM, AM-8  
     minimum requirements, AM-7  
     operating systems, AM-7  
     platforms, AM-7  
     uninstalling, AM-13  
 Account Management for Enterprise Console, GS-81  
 Account Unit  
     defined differently in AM Client and  
     FireWall-1, AM-55  
     description of, AM-4

## LEGEND

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLook GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

managing users on, WI-75  
 properties, AM-17  
 step by step instructions on how to use in Security Policy, AA-140  
 Account Unit Properties window  
 Encryption tab, AM-18  
 General tab, AM-17  
 accounting, AA-240, WI-214, OL-153  
 and synchronized FireWalls, AA-234  
 incompatible with FASTPATH, AA-325  
 ACE  
 configuring FireWall-1 to work with ACE software, AA-356  
 sdconf.rec file, AA-357  
 using DES option with FireWall-1, AA-365  
 Action Selection window, WI-231  
 active connections, AA-240, WI-215, OL-154  
 ActiveX, WI-123, OL-87  
 Additional Information Selection dialog box, OL-163  
 Additional Information Selection window, WI-233  
 additional reading, GS-26  
 add-on products, GS-81  
 address range, WI-61  
 defining, AA-177  
 Address Translation  
 and auxiliary connections, AA-321  
 and FTP PASV, AA-321  
 and SecuRemote, VP-91  
 communications between hosts in different internal networks, AA-196, AA-198  
 compound conditions, AA-176  
 configuring, AA-189  
 differences between the Command Line Interface and the GUI, AA-190  
 different configurations on different network objects, AA-216  
 explanation of fw\_x translation table, AA-215  
 FTP port command, AA-171  
 gateway with three interfaces, AA-194  
 gateway with two interfaces, AA-191  
 Hide mode, AA-158, AA-159  
 hiding the gateway's internal address, AA-211, AA-215  
 installing on selected hosts, AA-189  
 interaction with anti-Spoofing, AA-205  
 internal host with illegal IP address tries to communicate with external host with same IP address, AA-214  
 multiple translation, AA-176  
 need for, AA-155  
 PIX, AA-199  
 reply packets, AA-166  
 restrictions on rshell service, AA-171  
 restrictions on sqnet2 service, AA-171  
 restrictions on Xing service, AA-171  
 routing considerations, AA-165  
 Rule Base, AA-210  
 Static Destination mode, AA-164  
 Static Source mode, AA-162  
 translation both source and destination, AA-176  
 using with Encryption on the same system, AA-213  
 Address Translation configuration utility, AA-283  
 Address Translation Rules  
 generating automatically, AA-171  
 Address Translation tab, WI-158  
 Network Properties window, WI-33  
 Workstation Properties window, WI-30  
 administrators  
 adding or deleting, AA-225  
 AIX, see IBM AIX  
 alert command  
 anti spoof, WI-147  
 anti-spoof, WI-147, OL-114  
 mail, WI-147, OL-113  
 popup, WI-147, OL-113  
 SNMP, WI-147  
 SNMP Trap, WI-147, OL-113  
 User Authentication, WI-147, OL-114  
 user authentication, WI-147  
 user defined, WI-147, OL-113  
 alert.exe file, AA-376  
 alerts  
 received by, WI-207  
 sent to, WI-207  
 alias, AM-61  
 aliased interfaces, AA-363  
 America OnLine, AA-387  
 Anti Spoof Alert Command, WI-147

## LEGEND

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLook GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Index-ii FireWall-1 User Guide Master Index • September 1998

anti-spoof Alert Command, WI-147, OL-114  
 anti-spoofing, GS-99, WI-25, WI-48, OL-35, OL-47  
   compatibility with Address Translation, AA-205  
   example, WI-26  
   Interaction with Address Translation, AA-205  
 AOL, AA-387  
 application  
   silently dropping, WI-173, OL-132  
 Apply Gateway Rules to Interface Direction  
   property, AA-368  
 Apply Selection, WI-237, OL-165  
 Archie, OL-68  
 archie, AA-393  
 ARP, AA-233  
 aSERVERNAME.log file, AA-383  
 auth.C file, AA-377  
 auth.def file, AA-380  
 authenticated services  
   going across two or more FireWalls, AA-359  
 authentication  
   and synchronized FireWalls, AA-233  
   authentication methods, AA-28  
   authentication schemes, AA-30  
   comparison of different types, AA-29  
   re-authenticating an FWZ SecuRemote  
     connection, AA-151  
   transparent authentication, AA-28  
   when to use each type, AA-29  
 Authentication methods, AA-28  
 Authentication Passwords  
   synchronizing, AA-351  
 authkeys.C file, AA-379  
 authrules.C file, AA-379  
 Auto Scoping, WI-38, OL-39  
 auxiliary connections, AA-321  
 AXENT Pathways Defender, AA-30, AA-51, AM-48  
   defining as server, WI-101  
 AXENT Pathways SecureNet, AA-365

**B**  
 back connection  
   requested port, AA-321  
 back connections, AA-325, WI-85, OL-67  
   encrypting, VP-71

backup  
   backing up a Security Policy, AA-344  
 backward compatibility  
   Version 4.0 and earlier versions, GS-34  
 BackWeb, AA-322, AA-393  
 base.def file, AA-380  
 Basic Encryption Protocol, VP-133  
 Basic Session Key, VP-24  
 Bay Networks router, GS-8, GS-74, GS-77, GS-97,  
   WI-170, WI-197, OL-39, OL-139  
   defining network object as, WI-22, WI-41, OL-33  
   installing Encryption Module on, GS-77  
   installing FireWall-1 on, WI-36, OL-39  
   setup, WI-41, OL-41  
 before installing FireWall-1, GS-31  
 bibliography, GS-26  
 Big Indian, AA-315  
 Blackbox Properties, WI-48, WI-53  
 Block Intruder window, WI-216  
 Block Request window, WI-217  
 blocked system, restoring access to, AA-336  
 blocking connections, AA-269  
 boot process  
   protecting networks during, AA-319  
   protecting the gateway during, AA-320  
 bootp, AA-394  
 broadcast packets  
   prevent them from being identified as spoofed  
     packets, OL-37

**C**  
 cannot connect to the server  
   error message, AA-340  
 CD-ROM  
   location of files on, AM-8  
 certificate, AA-151  
 Certificate Authority, WI-106, VP-5  
   changing its public key, VP-71  
   ENTRUST, VP-46  
   function of, VP-5  
 Certificate Authority Keys window, VP-70  
 Certificate Discovery Protocol, VP-9  
 Certifying a Public Key, VP-5  
 chargen, AA-387, AA-394

## LEGEND

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLook GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Master Index

Index-iii

Check Point  
   home page, GS-29  
 checksum errors, WI-148, OL-114, VP-39  
 chkpnt.mib file, AA-382  
 Cisco, GS-8  
   fwtsicload, AA-273  
   setup, OL-40  
 Cisco PIX firewall  
   setup, WI-56, WI-57  
 Cisco router  
   defining network object as, OL-33  
   setup, WI-40  
 Client Authentication  
   authorizing services, AA-77, AA-82  
   configuring, AA-78  
   configuring support for HTTPS, AA-94  
   defining on a per-user rather than a per-group  
     basis, AA-357  
   logging, example of, AA-87  
   overview, AA-75  
   sign on methods, AA-76  
   signing on through a Web browser, AA-91  
   Single Sign On System Extension, AA-98  
   timeouts, AA-84  
   tracking, AA-83  
 Client Authentication Sign On Methods  
   fully automatic sign on, AA-77  
   manual sign on, AA-76  
   manual sign on through a Web browser, AA-91  
   manual sign on using TELNET, AA-87  
   partially automatic sign on, AA-76  
   using fully automatic sign on, AA-93  
   using partially automatic sign on, AA-92  
 Client Encryption  
   meaning of Destination, VP-90  
 CLIENT keyword  
   \$FWDIR/conf/masters file, AA-350  
 Client/Server deployment of Management  
   Module, AA-224  
 clients file, AA-377  
 clocks  
   synchronizing for SKIP, VP-132  
 code.def file, AA-380  
 color, AA-178, AA-179, WI-84, WI-87, WI-88,  
   WI-91  
 Column menu, WI-219  
 Column Selection menu, WI-225  
 comment, AA-178, AA-179, WI-84, WI-86, WI-87,  
   WI-88, WI-91, OL-72, OL-73  
   adding to a rule, WI-172  
 communication  
   between FireWall-1 components on different  
     machines, AA-345  
 compartmentalization  
   Account Units, AM-5  
 compatibility  
   Version 4.0 and earlier versions, GS-34  
 compiler, FireWall-1, AA-279  
 compiling a Security Policy, AA-257  
 conf/masters, AA-327, AA-341, AA-347  
 configuration  
   Security Servers, AA-123  
 configurations  
   managing distributed FireWall-1  
     configurations, AA-345  
 Conn. ID, WI-215, WI-217, OL-154, OL-155  
 Connected OnLine Backup, AA-387  
 connection to original-MTA failed  
   error message, AA-361  
 connections  
   blocking, WI-215  
   different routes for, AA-230  
   inhibiting or blocking, AA-269  
   lost when Security Policy re-installed, AA-345  
   terminating, WI-215  
 connections table, AA-322, AA-325  
 connections, enabling outgoing, OL-110  
 contains operator, AM-33  
 Content Vectoring Server, see CVP Server  
 control connection  
   accepting, WI-143  
   authentication and encryption, WI-143, OL-109  
   encrypting, AA-347  
 control information  
   sending to Kernel Module, AA-275  
 Control Properties, OL-107  
   displaying windows, WI-8, OL-21  
   interaction with Rule Base, OL-132

## LEGEND

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLock GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Index-iv FireWall-1 User Guide Master Index • September 1998

settings for SecuRemote Client, VP-92  
 Control Properties windows, OL-21  
 control.map, AA-348  
   access operations, list of, AA-349  
 control.map file, AA-380  
   modified during FireWall-1 reconfiguration, AA-345  
 CoolTalk, AA-322  
   enabling back connections, AA-388  
 cpp file, AA-376  
 creating an object in the LDAP directory, AM-24  
 creating groups, GS-34  
 crypt.def file, AA-380, VP-98  
 ctiver file, AA-384  
 CU-SeeMe, AA-394  
 CVP checking  
   URI resource, OL-87, OL-97, OL-100  
 CVP Inspection  
   step by step procedure, AA-133  
 CVP inspection  
   FTP resource, WI-131  
   SMTP resource, WI-127  
   URI resource, WI-123  
 CVP Server, AA-378, WI-98  
   defining, OL-78  
   how it is invoked, AA-129  
   step by step procedure for using, AA-133  
 CVP Server Properties window, WI-98, OL-78

## D

data field values  
   of rule, modifying, OL-130  
 date, AA-309  
 Date Selection Criteria window, WI-226  
 day, AA-309, OL-59  
 daytime, AA-388, AA-394  
 DB Download, WI-64, OL-56  
 DCE-RPC, AA-390, AA-397  
   required by MS Exchange, AA-322  
 DecNET  
   inspecting, AA-365  
 Decryption on Accept, OL-110  
 default directory  
   FireWall-1, GS-43  
 default rule, GS-91

default Security Policy, GS-66, AA-319, AA-320, AA-380  
   restrictions under IBM AIX, GS-59  
   verifying that it is loaded, AA-320  
 default.bin file, AA-384  
 default.fc file, AA-384  
 default.ft file, AA-384  
 default.lg file, AA-384  
 default.pf file, AA-380, AA-384  
 default.W file, AA-378  
 default\_server, WI-124, OL-98  
 default\_server parameter  
   smtp.conf, AA-111  
 defaultfilter, AA-380  
 defaultfilter.boot file, AA-380  
 defaultfilter.drop file, AA-380  
 deffunc, AA-311  
 define, AA-302, AA-311  
   difference between define and #define, AA-302, AA-311  
 DES  
   using ACE (SecurID) DES with FireWall-1, AA-365  
 Destination Selection window, WI-228, WI-230, OL-159, OL-164  
 dest-unreach, AA-398  
 Different Routes for Connections, AA-230  
 Diffie-Hellman scheme, VP-3  
 Digital Signature, VP-4  
 direction of enforcement, AA-367  
 directory  
   installing FireWall-1 in a directory other than the default directory, GS-43  
 discard, AA-388, AA-394  
 display.bat file, AA-376  
 displaying  
   System Status View Window, GS-11, GS-128, WI-202, OL-145  
 distributed FireWall-1 configuration  
   diagram, GS-36  
 distributed management  
   configuring FireWall-1 for, AA-345  
 DN  
   logging in using, AA-152  
 DNS, AA-388, OL-68

## LEGEND

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLook GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Master Index      Index-v



encryption in SecuRemote, VP-93, VP-97  
reverse resolving IP addresses using, OL-54

dns, AA-394

DNS, dual, AA-354

dnsinfo file, AA-378

dnsinfo.C file, AA-285

domain

defining properties of, OL-28, OL-53

load balancing algorithm, AA-237

using a domain object in a rule, WI-34, OL-53

Domain Name Download, WI-144, OL-111, OL-115

domain name download, enabling, WI-144, WI-149,

OL-111, OL-115

Domain Name Queries, WI-144, OL-111, OL-115

domain name queries, enabling, WI-144, WI-148,

OL-111, OL-115

Drop

differences from Reject, WI-167, OL-125

dropping an application, WI-173, OL-132

dup.def file, AA-380

## E

echo, AA-388, AA-394

echo-reply, AA-355, AA-398

echo-request, AA-355, AA-398

egp, AA-399

ebt\_set.C file, AA-380

Elapsed column

method of calculation, WI-214, WI-215, OL-153,

OL-154

embedded systems

where to install license, GS-69

Enable Domain Name Download, WI-144, WI-149

Enable Domain Name Queries, WI-144, WI-148

Enable ICMP, WI-144, WI-149, OL-108

Enable Outgoing Packets, WI-144

Enable Outgoing Packets property, AA-368

Enable Response of FTP Data Connections, WI-145,

OL-112

Enable RIP, WI-144, WI-148

Enable UDP Replies, WI-143

encapsulation

SecuRemote, VP-94

encryption

and synchronized FireWalls, AA-233

basic definitions, VP-1

changing keys, VP-32

communications with external networks, VP-30

configuration examples, VP-17

DNS, VP-97

incompatible with FASTPATH, AA-325

key hierarchy, VP-24

key management, VP-16

using with Address Translation on the same

system, AA-213

Virtual Encryption Session, VP-23

encryption algorithm

choosing for SecuRemote users, VP-59

encryption domain, VP-16

Encryption Module, GS-81

installing on Bay Networks and Xylan, GS-77

Encryption Properties window, VP-56

encryption rule

integrating in a Rule Base, VP-22

encryption scheme mismatch, WI-148, OL-114,

VP-39

End User License Agreement, AM-8

ends with operator, AM-33

Enforcement Point

definition of, GS-73

enforcing and installing, difference between, WI-173,

OL-133

enterprise ID, AA-242

ENTRUST Certificate Authority, VP-46, VP-122

Entrust Certificates, VP-122

Entrust Public Key Infrastructure, VP-45

Entrust users

creating profiles, VP-123

recovering profiles, VP-123

ENTRUST.INI file, VP-122

error message

"connection to original-MTA failed", AA-361

No Response from Server, WI-6

error\_server parameter

smtp.conf, AA-111

established TCP, WI-48, OL-47

established TCP connections, AA-322

enabling, OL-115

## LEGEND

AA Architecture and Administration

AM Account Management Client

GS Getting Started with FireWall-1

OL Managing FireWall-1 Using the OpenLook GUI

VP Virtual Private Networking with  
FireWall-1

WI Managing FireWall-1 Using the Windows GUI

Index-vi FireWall-1 User Guide Master Index • September 1998

established TCP packets, WI-147, OL-114  
 established TCP sessions, AA-322  
 evaluation license  
     ordering, GS-69  
 evaluation package  
     license for, GS-69  
 Excessive Log Grace Period, WI-146, OL-113  
 exec, AA-388  
 expiration, OL-59  
 expires, AA-303  
 explicitly defined rules  
     interaction with implicit rules, WI-177  
 Exportable  
     checkbox in Host Properties window, VP-87  
 Extended Encryption Protocol, VP-140  
 external FireWall Module  
     not managed by FireWall-1/n, GS-79, AA-365  
 external FireWalled object, WI-22, WI-32, WI-36,  
     WI-49, WI-54  
 external group, AA-141  
     creating, WI-75  
     deleting, WI-78  
     modifying, WI-78  
     when changes take effect, WI-75, WI-78  
 external interface  
     hiding IP address, AA-159, VP-86  
     not set by this loading  
         error message, AA-337  
     of gateway, specifying for ISAKMP/  
         OAKLEY, GS-33, VP-28  
     of gateway, specifying for SKIP, VP-25  
     reconfiguring, AA-337  
     specifying IP address of, VP-131  
 external interfaces  
     restricted in FireWall-1/n, GS-79, AA-364  
 external users  
     managing, WI-74  
 external.if file, AA-337, AA-378  
     modified during FireWall-1 reconfiguration, AA-345  
  
**F**  
 Fast mode, WI-85, OL-67  
 Fastpath, WI-85, OL-67  
 fault tolerance, AA-373  
 Fetch command (Named Masks window), WI-182  
  
 field, data  
     modifying value of, OL-130  
 Find Date, WI-222  
 Find in all Fields window, WI-223  
 Find menu, WI-223  
 Find window, WI-222  
 finger, AA-388  
 FireWall, GS-76, AA-221  
 FireWall daemon  
     stopping, AA-256  
 FireWall Inspection Components, AA-292  
 FireWall Module, GS-81  
     description of, AA-223  
     minimum requirements (Windows), GS-40  
     starting, AA-256  
 FireWall Module and Inspection Module, differences  
     between, GS-76, AA-221  
 FireWall Modules  
     restrictions on synchronization, AA-232  
 FireWall Synchronization  
     example, AA-230  
     implementation, AA-230  
 FireWall synchronization  
     overview, AA-229  
 FireWall-1  
     administrative issues, AA-369  
     before installing, GS-31  
     configuration, AM-3  
     Home Page, GS-29  
     installing in a directory other than the default  
         directory, GS-43  
     killing the daemon and fw stop, difference  
         between, AA-369  
     mailing list, GS-29  
     performance, GS-24  
     reconfiguring, AA-254, AA-255  
     stopping, AA-369  
     uninstalling, GS-68  
     upgrading to a new version of, GS-34  
     Web Page, GS-29  
 FireWall-1  
     disabling (NT), GS-54  
     loss of state after upgrading, GS-35  
     reconfiguring (NT), GS-55

## LEGEND

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLook GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Master Index

Index-vii

stopping (NT), GS-54  
 stopping inspection (NT), GS-54  
 uninstalling (NT), GS-54  
 uninstalling (Unix), GS-68  
 FireWall-1 Adapter  
   removing, VP-110  
   restrictions on adding and removing, VP-93  
 FireWall-1 authentication password  
   installing, AA-261  
 FireWall-1 components on different machines  
   communication between, AA-345  
 FireWall-1 Control Connections, OL-109  
 FireWall-1 daemon  
   sending signal to, AA-278  
 FireWall-1 driver  
   loading process, AA-404  
 FireWall-1 FireWall daemon  
   stopping, AA-256  
 FireWall-1 FireWall Module  
   starting, AA-256  
 FireWall-1 HP OpenView Extension  
   installing, AA-244, AA-245, AA-246  
   specifying the Management Server for FireWalled  
   objects, AA-247  
 FireWall-1 HP OpenView extension  
   default SNMP port for FireWalled objects, AA-246  
   FireWall discovery, AA-246  
 FireWall-1 license, see license  
 FireWall-1 password  
   advantage over OS password, AA-30  
 FireWall-1 SNMP daemon, AA-241  
 FireWall-1 software  
   installation problems, GS-67  
   reconfiguring, GS-68  
   upgrading, GS-67  
 FireWall-1 version number  
   displaying, AA-267  
 FireWall1, upgrading to a new version of  
   objects carried over from previous version, GS-34  
 FireWall-1/n products  
   restrictions, GS-79, AA-364  
 FireWall-1 license  
   installing, GS-69  
   obtaining, GS-69  
 FireWalled gateway  
   definition of, GS-73  
 FireWalled host  
   definition of, GS-73  
   displaying status of, AA-264  
 FireWalled, defined, GS-4  
 first IP address, AA-177  
 first port, AA-178  
 format file  
   name displayed in status bar, WI-213  
 format lists, AA-308  
 formats.def file, AA-380  
 free function, AA-303  
 FreeTel, AA-322, AA-394  
 FTP, GS-18, AA-29, AA-321, AA-325, WI-85,  
   OL-67  
   authenticated session, description of, GS-19  
   authenticating through the HTTP Security  
   Server, AA-358  
   back connection, AA-345  
   back connections, encrypting, VP-71  
   data connection, AA-345  
   data connection, enabling response of, WI-145,  
   OL-112  
   file names logged for authenticated  
   sessions, AA-103, WI-218, OL-155  
   from HTTP, AA-355  
   get and put logged for User Authenticated  
   FTP, AA-103  
   PORT command, AA-345  
   User Authentication, GS-18, AA-29  
   using with SecuRemote Client, VP-92  
 ftp, AA-388  
 ftp back connections  
   encrypting, VP-71  
 FTP daemon, AA-356  
 FTP data connections, AA-321, AA-388, WI-145  
 FTP PASV, AA-321  
   enabling FTP Passive Connections, WI-145,  
   OL-112  
 FTP PASV connections, OL-112  
 FTP proxy  
   defining to browser, AA-355, AA-358  
 FTP resource  
   CVP inspection, WI-131

#### LEGEND

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLook GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Index-viii FireWall-1 User Guide Master Index • September 1998

matching, AA-108  
 FTP resources  
   command matching, AA-108  
   file name matching, AA-108  
   matching, AA-108  
 fw command, AA-256  
 fw converthosts, AA-285  
 fw cti, AA-275  
 fw dbimport, AA-287  
 fw fetch command, AA-259  
 fw file, AA-376  
 fw gen command, AA-278  
 fw kill, AA-383  
 fw lchosts command, AA-265  
 fw log command, AA-265  
 fw logswitch command, AA-260  
 fw printlic, AA-262  
 fw printlic command, AA-268  
 fw putkey, AA-261, AA-341, AA-351  
 fw putlic command, AA-261, AA-262  
 fw sam command, AA-269  
 fw stat command, AA-264  
 fw tab command, AA-283  
 fw unload command, AA-259, AA-265, AA-267  
 fwalog file, AA-383  
 fwalogptr file, AA-383  
 fw.conf file, AA-383  
 fwinfo file, AA-380  
 fw.license file  
   modified during FireWall-1 reconfiguration, AA-345  
 fw.log file, AA-383  
 fw.logptr file, AA-383  
 fw.logtrack file, AA-383  
 fw.mkdev file, AA-383  
 fw.sys file, AA-383  
 fw.vlog file, AA-383  
 fw.vlogptr file, AA-383  
 FW1\_clntauth, AA-97  
 fw1allowed-dst, AA-148, AM-39  
 fw1allowed-src, AA-148, AM-39  
 fw1allowed-vlan, AA-148, AM-39  
 fw1authmethod, AA-146, AM-37  
 fw1auth-server, AA-147, AM-38  
 fw1day, AA-148, AM-39  
 fw1enc-fwz-expiration, AA-148, AM-39  
 fw1expiration-date, AA-148, AM-39  
 fw1groupTemplate, AA-149, AM-40  
 fw1hour-range-from, AA-148, AM-39  
 fw1hour-range-to, AA-148, AM-39  
 fw1person, AM-34, AM-35  
 fw1pwdLastMod, AA-147, AA-151, AM-38  
 fw1Skey-mdm, AA-147, AM-38  
 fw1Skey-passwd, AA-147, AM-38  
 fw1Skey-seed, AA-147, AM-38  
 fw1sr-auth-track, AA-149, AM-40  
 fw1SR-datam, AA-148, AM-39  
 fw1SR-keym, AA-148, AM-39  
 fw1SR-mdm, AA-148, AM-39  
 fw1template, AM-35  
 fwal, AA-262  
   definition of, AA-349  
 fwal authentication, AA-350  
 fwalert file, AA-376  
 fwauth.keys file, AA-378  
   modified during FireWall-1 reconfiguration, AA-345  
 fwauth.NDB file, AA-378, AA-379  
 fwauth.NDB7 file, AA-378  
 fwauth.NDBBK7 file, AA-378  
 fwauthbd.conf, AA-97  
 fwauthbd.conf file, AA-378  
   modified during FireWall-1 reconfiguration, AA-345  
 fwav file, AA-376  
 fwav.conf file, AA-378  
 fwavstart file, AA-376  
 fwavstop file, AA-376  
 fwc, AA-279  
 fwc file, AA-376  
 fwdisco file, AA-376  
 fwdiscoload, AA-273  
 fwdiscoload file, AA-376, AA-377  
 fwcmd.exe file, AA-376  
 fwcomp file, AA-376  
 fwconfig  
   installing a license using, AA-262  
 fwconfig file, AA-376  
 fwconn.h file, AA-380  
 fwctrnm.h file, AA-380  
 fwctrs.h file, AA-380

## LEGEND

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLook GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Master Index

Index-ix

fwctrs.ini file, AA-380  
 fwd file, AA-376  
 fwd.h file, AA-337  
 fwd.hosts file, AA-337  
 fwd.pid file, AA-384  
 FWDIR  
   importance of setting correctly, GS-43  
 fwell file, AA-376, AA-385  
 fwf2htbin.gif file, AA-380  
 fwf2htdir.gif file, AA-380  
 fwf2htunknown.gif file, AA-380  
 fwinfo debugging tool  
   incorrect functioning, GS-43  
 fwinfo file, AA-376  
 fwinfo.pmr file, AA-376  
 fwinfo2 file, AA-376  
 fwinstall file, AA-376  
 fwiv file, AA-376  
 fwiv.info file, AA-380  
 fwm file, AA-376  
 fwm.pid file, AA-384  
 fwmod.\* files, AA-383  
 fwmusers file, AA-378  
 fwntperf.dll file, AA-381  
 fwopsec.conf file, AA-271, AA-378  
 fwrl.conf file, AA-378  
 fwrlconf file, AA-384  
 fwsngui file, AA-376  
 fwsnmp.dll file, AA-381  
 fwstart, GS-59, AA-234, AA-277  
 fwstart file, AA-376  
 fwstop, GS-59, AA-277, AA-383  
   and killing the FireWall-1 daemon, difference  
     between, AA-369  
 fwstop file, AA-376  
 fwui file, AA-376  
 fwui.log file, AA-383  
 fwui\_head.def file, AA-381  
 fwui\_trail.def file, AA-381  
 fwuninst file, AA-376  
 fwuninstall file, AA-376  
 fwuserauth.NDB file, AA-379  
 fw\_x\_translation table  
   explanation of fields in, AA-215

fwxauth file, AA-377  
 fwdconf, AA-189, AA-283  
 fwdconf file, AA-377

## G

gateway  
   cannot connect through, AA-335  
   defining network object as, WI-22, OL-33  
   defining properties of, OL-23, OL-28, OL-83  
   getting its key before installing a Security Policy on  
     it, VP-53, VP-54  
   hiding IP address of external interface, AA-159,  
     VP-86  
   specifying communication direction of rules  
     on, WI-142, OL-109  
 gateway, protecting, GS-91  
 gateways  
   defining interfaces as separate objects, AA-355  
   direction of enforcement on, AA-368  
 generic services  
   service properties, WI-88, OL-73  
 generic user, AA-325, WI-72, OL-61  
 ggp, AA-399  
 Global Pool, AA-201  
 gopher, AA-388  
 GoTo Menu, OL-169  
 gps.pro file, AA-381  
 grace period between logs of similar packets, OL-113  
 greater than operator, AM-33  
   compatibility with LDAP versions, AM-33  
 group  
   form of DN, AM-59  
 groups  
   adding elements to, OL-57, OL-65  
   defining properties of, OL-28  
 GUI Client  
   minimum requirements, GS-39, VP-105  
 GUI Clients  
   adding or deleting, AA-224  
 GUI windows  
   closing, WI-8, OL-21  
   displaying, WI-8, OL-21  
 gui-clients file, AA-378

## LEGEND

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLook GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Index-x FireWall-1 User Guide Master Index - September 1998



**H**

H.323, AA-322, AA-325, AA-389, WI-85, OL-67  
 enabling back connections, AA-389  
 hashsize, AA-303  
 heuristic check of Rule Base, WI-173, OL-131  
 hidden rules, WI-178  
   displaying, WI-179  
   unhiding, WI-179  
 Hide mode, AA-159  
 Hide Repeating Lines option, OL-165  
 Hide/Unhide menu, WI-219  
 hiding IP addresses, AA-369  
 hiding rules, WI-178  
 High Availability, AA-229  
   encrypting connections between synchronized  
     FireWalls, AA-233  
   SKIP, AA-233  
   synchronizing different version FireWall  
     Modules, AA-233  
   synchronizing FireWall Modules on different  
     platforms, AA-232  
   synchronizing FireWall Modules with different  
     Security Policies, AA-233  
 high availability  
   Account Units, AM-5  
 hijacking sessions, AA-363  
 HKEY\_LOCAL\_MACHINE, AA-401  
 hostname command, AA-353, VP-131  
 hosts  
   defining network objects as, WI-22, OL-33  
   defining properties of, OL-23, OL-28  
   direction of enforcement on, AA-368  
   list of those protected by FireWall-1/n  
     product, AA-265  
 hosts file, GS-33, AA-370, WI-22, WI-36, OL-28,  
   OL-38  
 Hosts, Gateways and Interfaces  
   distinction between, AA-353  
 hour, OL-59  
 HP  
   FireWall-1 HP OpenView extension, AA-243  
 HP OpenView, see FireWall-1 HP OpenView extension  
 HP-UX 10  
   transitional links option, GS-56

HTML, AA-380

HTML Weeding, WI-123

HTML weeding, AA-380

HTTP

allowing FTP sessions from, AA-355

blocking JAVA applets, OL-87

restricting inbound, AA-48

  restricting internal user's access to JAVA  
  applets, OL-87

restricting outbound, AA-48

User Authentication, GS-18, AA-29

using a Server for Null Requests, AA-60

using reauthentication options, AA-47

http, AA-388

HTTP Authenticating Server

blocking JAVA applets, OL-87

HTTP Security Server

as proxy, AA-112

configuring multiple ports, AA-56

defining as a Security Proxy, AA-51

defining as an HTTP proxy, AA-50

error messages, AA-56

overview, AA-44

putting a proxy behind, AA-45

support for FTP, AA-112

support for HTTPS, AA-113, AA-116

HTTP Servers

defining, AA-46

HTTPS, AA-366

authenticating outbound, AA-51

using URI Resource rules with, AA-116

with non-transparent authentication, AA-60

https, AA-388

**I**

IANA, AA-170, AA-366

IBM AIX

IP Forwarding, GS-59

overwriting previous installation, GS-59

separate JRE installation, AM-13

X/Motif library version, GS-59

license

overwriting, AA-263

ICMP, WI-144, WI-145, OL-111

**LEGEND**

AA Architecture and Administration

AM Account Management Client

GS Getting Started with FireWall-1

OL Managing FireWall-1 Using the OpenLook GUI

VP Virtual Private Networking with  
FireWall-1

WI Managing FireWall-1 Using the Windows GUI

Master Index

Index-xi

accepting, OL-116  
 enabling, WI-144, WI-149, OL-111, OL-116  
 match string, WI-88, WI-89, OL-72, OL-73  
 ICMP Redirect  
   enabling, WI-145, WI-149, OL-111, OL-116  
 ident, AA-389  
 igrp, AA-399  
 imap, AA-389  
 implicit drop rule, GS-91  
 implicit rules  
   interaction with explicitly defined rules, WI-177  
   toggling display of, WI-10  
 Implied Pseudo-Rules option on View menu, WI-178  
 implies, AA-303  
 in.aclientd file, AA-377  
 in.ahptd file, AA-377  
 in.ahptd file, AA-377  
 in.ariogind file, AA-377  
 in.asmtpd file, AA-377  
 in.atelentd file, AA-377  
 in.lhttpd file, AA-377  
 in.telnetd, AA-356  
 incoming communications  
   Security Policy enforced on, AA-367  
 inetd.conf, AA-356  
 inetOrgPerson, AM-34, AM-35  
 Info field  
   get and put logged for authenticated FTP, WI-218,  
   OL-155  
 info-reply, AA-398  
 info-req, AA-398  
 inhibiting connections, AA-269  
 init.def file, AA-381  
 inode, AA-383  
 inside net, WI-59, OL-52  
 INSPECT  
   accept, AA-310  
   backwards compatibility, AA-311  
   call, AA-311  
   compatibility between FireWall-1 versions, AA-311  
   compiler, AA-279  
   compound conditions, AA-294  
   constants, AA-299  
   current packet, AA-310  
   date, AA-309  
   day, AA-309  
   day in month specification, AA-300  
   day in week specification, AA-300  
   delete, AA-306  
   direction, AA-310  
   drop, AA-312  
   dynamic tables, AA-304  
   elements of a rule, AA-295  
   expcall attribute, AA-305  
   expires attribute, AA-305  
   export, AA-312  
   format lists, AA-308  
   function definitions, AA-311  
   get, AA-304  
   hex, AA-308  
   hold, AA-313  
   host, AA-310  
   identifier names, AA-301  
   ifaddr, AA-310  
   in, AA-313  
   include files, AA-298  
   Install On, AA-296  
   int, AA-308  
   interface, AA-310  
   IP address constant, AA-300  
   ipaddr, AA-308  
   keep attribute, AA-305  
   limit attribute, AA-305  
   lists, AA-307  
   log, AA-313  
   LOG macro, AA-316  
   macros, AA-316  
   modify, AA-306, AA-314  
   name resolution, AA-301  
   netof, AA-314  
   nexpres attribute, AA-305  
   numeric constants, AA-299  
   operators, AA-309  
   packetid, AA-310  
   port, AA-308  
   pre-processor, AA-300  
   preprocessor, AA-316  
   proto, AA-308

## LEGEND

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLock GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Index-xii FireWall-1 User Guide Master Index • September 1998



record, AA-306, AA-314  
 refresh attribute, AA-305  
 reject, AA-314  
 reserved words, AA-299  
 rule, elements of, AA-295  
 scope, AA-296  
 segment register, AA-301  
 service, AA-308  
 set, AA-314  
 static tables, AA-307  
 string, AA-308  
 tables, AA-302  
 time specification, AA-299  
 tod, AA-309  
 track, AA-296  
 TRAP macro, AA-316  
 uint, AA-308  
 vanish, AA-315  
 INSPECT tables  
   displaying, AA-283  
 Inspection Code  
   compiling from Inspection Script, WI-174, OL-133  
   installing, AA-317, OL-138  
 Inspection Code Loading, WI-196, OL-61, OL-139  
 Inspection Module  
   architecture, GS-13  
   defined, GS-4  
   fetching last installed on host, AA-259  
   network objects allowed to load, AA-378  
 Inspection Module and FireWall Module, differences  
   between, GS-76, AA-221  
 Inspection Module tables, displaying, using command-  
   line interface, AA-283  
 Inspection Script  
   backwards compatibility, AA-311  
   compiling, AA-279, AA-317  
   compiling Inspection Code from, WI-174, OL-133  
   generating from Rule Base, AA-278  
   generating using command-line interface, AA-278  
   manually editing, WI-174, OL-133  
   viewing, WI-194, OL-137  
   writing, AA-292  
 Install On field  
   NAT tab, AA-173  
 installation  
   HP-UX, AM-10  
   IBM AIX, AM-12  
   Solaris, AM-9  
   Unix, AM-9  
   Windows, AM-8  
 installing  
   router access list, WI-200, OL-142  
   Rule Base on hosts, OL-148  
   Security Policy, WI-193  
 installing a FireWall-1 authentication  
   password, AA-261  
 installing a FireWall-1 license, GS-69  
 installing a FireWall-1 license, AA-262  
 installing and enforcing, difference between, WI-173,  
   OL-133  
 installing FireWall-1, GS-31  
 installing the Account Management Client, AM-8  
 Insufficient Information problem, AA-104  
 Integrated FireWalls  
   general properties, WI-53  
   PIX setup, WI-56  
   TimeStep setup, WI-55  
 Integrated Firewalls, WI-52  
 interface data  
   fetching automatically, WI-24  
 Interface names  
   Bay routers, AA-222  
 Interface Selection Criteria window, WI-227  
 Interface Selection dialog box, WI-227, OL-158  
 interfaces  
   aliased, AA-363  
   defining a gateway's interfaces as separate  
     objects, AA-355  
   defining as an object, AA-355  
   how Security Policy is enforced on  
     different, AA-367  
   network, properties of, WI-24, OL-33, OL-40  
   result of failing to define, WI-23, WI-24, OL-34  
   virtual, AA-363  
 interfaces, external  
   restricted in FireWall-1/50 and FireWall-1/  
     250, GS-79, AA-364, AA-365  
 internal FireWalled object, WI-22, WI-32, WI-36,  
   WI-49, WI-54

## LEGEND

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLook GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Master Index

Index-xiii

- internal hosts
  - number restricted in FireWall-1/n, GS-79, AA-364
  - too many, AA-337
- internal interfaces
  - not restricted in FireWall-1/n, GS-79, AA-364
- internal network objects, WI-64, OL-24, OL-84
- Internal password, AM-48
  - advantage over OS password, AM-48
- Internet
  - defining to FireWall-1, AA-352
- InternetPhone, AA-394
- intrap, AA-303
- intruders
  - blocking connections from or to suspected, WI-215
- IP Address, WI-32, WI-49
- IP addresses
  - hiding, AA-369
  - resolving updated, if modified, OL-171
  - unregistered, AA-369
  - when does changing take effect, AA-345
  - which to use when directing logging to, AA-328
- IP Forwarding, GS-34, AA-275
  - controlling status of with FireWall-1, AA-275
  - enabling and disabling, AA-276
  - enabling and disabling on HP-UX 10, AA-276
  - enabling and disabling on IBM AIX, AA-277
  - enabling and disabling on Solaris 2, AA-276
  - enabling and disabling on Windows NT, AA-277
  - IBM AIX, GS-59, AA-275, AA-277
- IP Options, AA-363, WI-147
  - track dropping of, OL-114
- IP Tunnels, WI-43
- IPSec
  - reply packets not returning, VP-131
- IPSec session key
  - expiration in the course of an encrypted session, VP-38
- IPX
  - inspecting, AA-365
- IPX packets
  - inspecting, AA-365
- irc, AA-389
- is not operator, AM-33
- is operator, AM-33
- ISAKMP, AA-394
  - reply packets not returning, VP-131
- ISAKMP negotiations
  - logging, VP-38
- ISAKMP SA
  - expiration in the course of an encrypted session, VP-38
- ISAKMP/OAKLEY
  - specifying the encrypting gateway's IP address, GS-33, VP-28
- ISDN interfaces, AA-366
- J**
  - JAVA, WI-123, OL-87
    - blocking JAVA applets, WI-123, OL-87
  - Java
    - separate installation for IBM AIX, AM-13
    - version required for Account Management Client, AM-13
  - JAVA applets
    - already in cache, WI-123, OL-87
  - Java Runtime Environment, see JRE
  - JAVA Script, WI-123, OL-87
  - JRE
    - installing on IBM AIX, AM-13
- K**
  - kbuf, AA-303
  - keep, AA-303
  - Kerberos, AA-365
  - kerberos, AA-389, AA-394
  - Kernel Module
    - sending control information to, AA-275
  - kerntabs.h file, AA-381
  - kertabs.def file, AA-381
  - keys
    - fetching over Internet, VP-26, VP-30, VP-48, VP-49, VP-53, VP-54, VP-71
- L**
  - last IP address, AA-177
  - last port, AA-178
  - LDAP, WI-74
    - Account Unit, AA-139, AA-140, AM-4
    - defining users in both LDAP and

**LEGEND**

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
CL Managing FireWall-1 Using the OpenLook GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Index-xiv FireWall-1 User Guide Master Index • September 1998

- FireWall-1, AA-142, AA-154
- exporting users from the FireWall User Database, AA-152
- port number for SSL connection, WI-106, AM-1
- port number for standard connection, AM-1
- schema checking, AA-153
- security issues, AA-153
- version with which FireWall-1s compliant, AA-152
- LDAP Account Unit
  - step by step instructions on how to use in Security Policy, AA-140
- LDAP Server
  - enabling connections from FireWall Module to, OL-109
  - SSL, AM-18
- LDAP server, see also Account Unit
- LDAP servers
  - indexing, AA-153
  - optimizing, AA-153
- ldap service, AA-389
- LDAP Version 2.0, AA-152
- LDAP Version 3.0, AA-152, AM-18, AM-33
- LDAP servers
  - defining, WI-102
- ldap-ssl, AA-389
- LDIF syntax, AA-288
- less than operator, AM-33
  - compatibility with LDAP versions, AM-33
- libsun\_av.so file, AA-381
- license
  - confirming that you are using correct licenses, GS-70
  - deleting, AA-263
  - displaying, AA-268
  - for evaluation package, GS-69
  - installing, GS-69, AA-262
  - installing on host, AA-261, AA-262
  - obtaining, GS-68
  - printing, AA-268
  - reconfiguring with fwconfig, GS-61, AA-255
  - removing, AA-263
  - removing old licenses, GS-69
  - where to install, GS-68
  - where to install for embedded systems, GS-69
- license.rtf, AM-8
- license.txt, AM-8
- limit, AA-303
- Little Endian, AA-315
- live connections, AA-240, OL-154
- LiveLan, AA-389
- lmhosts file, GS-33, AA-370, WI-22, WI-36, OL-28, OL-38
- Load Agents
  - defining parameters, WI-155, OL-121
- Load Agents Port property, AA-240
- Load Balancing, AA-234
  - defining parameters, WI-155, OL-121
  - step by step instructions, AA-237
- load balancing algorithms, AA-236
- Load Measurement Interval property, AA-240
- Load Measuring, AA-239
- load\_agent file, AA-377
- loading a Security Policy, AA-257
- local.arp, AA-384
- local.arp file, AA-168
- locking, AA-383
- locking mechanism
  - used to prevent simultaneous updates, AA-225
- lockmanager, AA-397
- Log
  - rule number zero, AA-362
  - rule with negative number, AA-362
- log
  - established TCP packets, AA-324
  - grace period between similar packets, OL-113
  - printing, WI-239, OL-172
  - redirect logging to another Master, AA-327
  - saving, WI-239, OL-172
  - scrolling, WI-222, OL-157
  - viewing, WI-211, OL-151
- Log entries, selecting by
  - additional information, WI-233
  - destination, WI-227
  - DstKeyID, WI-233
  - information, WI-233
  - interface, WI-227
  - number, WI-226
  - origin, WI-227

## LEGEND

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLook GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Master Index

Index-xv

port, WI-226  
 rule, WI-226  
 service, WI-227  
 source, WI-227  
 SrcKeyID, WI-233  
 type, WI-230  
 user, WI-227

Log File  
 creating new, AA-260  
 deleting, WI-239  
 displaying contents of, AA-265  
 exporting, AA-266, WI-240  
 miscellaneous functions, WI-239  
 name displayed in title bar, WI-213  
 opening another, WI-238  
 printing, WI-239  
 reload, WI-240  
 saving, WI-239  
 starting a new, WI-239  
 stop updating, WI-240

log file  
 analysis of, AA-362  
 creating new, OL-171  
 creating new, using command-line  
 interface, AA-260  
 deleting, OL-171  
 displaying, using command-line interface, AA-265,  
 AA-269  
 exporting to ASCII file, AA-266  
 managing, WI-238, OL-171  
 navigating and searching in, WI-222, OL-169  
 periodically switching, AA-363  
 saving, WI-239, OL-172  
 searching for a text string in, WI-223, OL-170  
 statistical analysis of, AA-362

LOG macro, AA-316

Log Server  
 definition of, WI-212

Log Viewer, GS-128, WI-211, OL-151  
 displaying, WI-8, OL-21  
 hiding data fields, OL-157  
 nothing in, AA-340  
 selection criteria, WI-225, OL-157

logging

Access Control, AA-225  
 packets as dropped though connection  
 continues, AA-324  
 redirecting to additional Masters, AA-327  
 redirecting to another Master, AA-327  
 when the FireWalled Gateway is not the Management  
 Station, AA-327  
 where to direct, AA-378

Logging and Alerting  
 Security Policy, WI-146, OL-113, VP-38

Logical Servers, AA-237  
 step by step instructions on using, AA-237  
 using HTTP Logical Servers in rule, AA-239

logical servers, WI-61, OL-25  
 persistent server mode, AA-238

login, AA-389  
 with DN or user name, AA-152

logviewer.C file, AA-378

Lotus Notes, AA-389

## M

Mail Alert Command, WI-147, OL-113

manage.lock file, AA-225, AA-383

Management Module  
 definition of, GS-74  
 description of, AA-223

Management Point  
 definition of, GS-74

Management Server, AA-279  
 definition of, GS-74  
 description of, AA-224  
 minimum requirements (Unix), GS-55  
 minimum requirements (Windows), GS-39  
 name displayed in status bar, WI-213  
 name of executable, AA-224  
 problems in connecting to, WI-5  
 timeout in connecting to, WI-6

Management Station  
 definition of, GS-74

Managing 3Com Filters  
 routers, WI-47, OL-46

mangling  
 packets of an established TCP connection, AA-315,  
 AA-323, AA-324

## LEGEND

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLook GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Index-xvi FireWall-1 User Guide Master Index • September 1998

- masking rules, WI-178
- mask-reply, AA-398
- mask-request, AA-398
- masks
  - applying, WI-183
- Master
  - defining a network object as, AA-378
  - fetching Security Policy from, AA-259
  - redirect logging to additional Masters, AA-327
  - redirect logging to another Master, AA-327
  - redirecting logging to another Master, WI-239
  - which IP address to use when directing logging to, AA-328
- MASTERS
  - parameter in control.map file, AA-348
- masters file
  - description of, AA-378
  - modified during FireWall-1 reconfiguration, AA-345
- MASTERS keyword
  - \$FWDIR/conf/masters file, AA-348
- match, WI-88, WI-89, OL-72
- memory usage, AA-372
- MIB, AA-242
  - chkpnt.mib file, AA-242
  - chkpnt.mib file source code, AA-248
  - location, AA-382
  - mib.txt file, AA-382
  - mib.txt2 file, AA-382
  - RFC support, AA-241
  - Wellfleet, AA-385
- mib.txt file, AA-382
- Microsoft Conferencing, AA-389
- Microsoft Exchange, AA-390
- Microsoft NetMeeting, AA-390
- Microsoft NetShow, AA-390
- Microsoft RRAS, WI-44
- Microsoft SQL Server, AA-390
- MIME
  - stripping specified types of attachments from message, WI-126, OL-97
- MIME attachments
  - definable in an SMTP Resource, WI-126, OL-97
  - definition syntax in SMTP Resource, WI-126, OL-97
- minimum requirements
  - Account Management Client, AM-7
  - FireWall Module, GS-40
  - FireWall Module (Windows), GS-40
  - FireWall-1 (Unix), GS-55
  - GUI Client, GS-39
  - GUI client, GS-39, VP-105
  - Management Server, GS-39, GS-55, AM-7
  - Management Server (Unix), GS-55
  - Management Server (Windows), GS-39
  - SecuRemote Client, VP-105
  - Unix platforms, GS-55
- modem connections
  - securing, AA-364
- modtrap, AA-303
- monitoring system status, GS-128, WI-201, OL-145
- Mosaic, AA-390
- mountd, AA-397
- MS Exchange, AA-322
- multicast, AA-367
- multiple adapters, VP-109
- N**
  - name, AA-177, AA-178, AA-394, WI-84, WI-86, WI-87, WI-88, WI-91, OL-72, OL-73
  - named, WI-144, WI-149
  - nbdatagram, AA-394
  - nbname, AA-394
  - nbssession, AA-390, WI-48, OL-47
  - NET, AA-390
  - NDIS3.1, VP-103
  - negate rules, WI-47, OL-46
  - net mask, WI-32
  - NetBEUI, see NET
  - NetShow, AA-322
  - netstat, AA-390
  - network configuration
    - modifying, VP-109
  - network interface properties, WI-24, OL-33, OL-40
  - network object
    - creating, GS-108, GS-121, GS-122, WI-18
    - creating groups of network objects, WI-59
    - defining, WI-15, OL-23, OL-75, OL-83
    - defining properties of, OL-23, OL-28, OL-83

**LEGEND**

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLook GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Master Index

Index-xvii



deleting, WI-19, OL-27, VP-67  
 editing existing, WI-19, WI-96, OL-26, OL-84  
 group, WI-59, WI-107, WI-139, OL-81,  
     OL-106  
 group, adding service to, WI-91  
 group, defining properties of, WI-68, OL-65,  
     OL-102  
 group, deleting service from, WI-92  
 internal, WI-64, OL-24, OL-84  
 modifying, WI-19  
 properties, WI-15, WI-93, WI-94, OL-23,  
     OL-75, OL-83, OL-103  
 network object group  
     deleting from, WI-60  
 network object properties  
     resolving updated, if modified, OL-171  
 network objects  
     limit of 240 objects in XView menu, OL-32  
     which are on my network?, AA-352  
 Network Objects Manager, OL-24, OL-84  
     displaying, WI-8  
 Network Objects Manager window, OL-20  
 NFS, AA-397  
 nfsd, AA-394  
 nfsprog, AA-397  
 NIS, AA-397  
 nisplus, AA-397  
 nntp, AA-390  
 node  
     definition of, GS-74  
 nodes  
     number restricted in FireWall-1/n, GS-79, AA-364  
 Non-Transparent Authentication  
     and HTTP, AA-58  
 Non-transparent Authentication  
     prompt\_for\_destination parameter, AA-43  
 Notify Sender on Error field, AA-361  
 NT and Unix  
     syntax differences, AA-253  
 ntp, AA-391, AA-395  
 Number Selection Criteria window, WI-226  
  
**O**  
 object  
     creating in LDAP directory, AM-24  
     objects.C file, AA-43, AA-378, AA-379  
     omi.conf file, AA-379  
     On Line option, OL-165  
     one-time passwords, VP-121  
     OnTime, AA-395  
     Open Platform for Secure Enterprise Connectivity, see  
         OPSEC  
     Open Security Extension, GS-81  
     Open Windows, AA-391  
     OpenView, see FireWall-1 HP OpenView extension  
     OPSEC, AA-128, AA-133  
     OPSEC-certified products  
         obtaining evaluation copies, AA-128, AA-133  
     Options window, WI-237  
     options.conf file, AA-379  
     organization, AM-25  
     Organizational Unit  
         creating, AM-24  
     organizationalPerson, AM-34, AM-35  
     organizationalUnitName, AM-24  
     OS Password, AM-47  
     ospf, AA-399  
     outgoing communications  
         Security Policy enforced on, AA-367  
     outgoing connections, enabling, OL-110  
     outgoing packets  
         accepting, WI-144  
     outtrap, AA-303  
     Overview, GS-4, AM-1  
     overwriting previous AIX installation, GS-59  
  
**P**  
 packet filter  
     Installing Security Policy on, WI-197, OL-139  
 Packet Key, VP-24  
 packet reassembly, AA-363  
     security risks associated with, AA-363  
 param-prblm, AA-398  
 password  
     echoing, VP-121  
     erasing, VP-121  
     expiration, VP-121  
     limitation on length in Windows, GS-48

## LEGEND

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLook GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Index-xviii FireWall-1 User Guide Master Index • September 1998

verifying, AA-146, AM-37  
 password expiration, AA-151  
 PASV  
   enable FTP PASV, WI-145  
   enabling FTP Passive Connections, WI-145, OL-112  
 pcnfsd, AA-397  
 Perfect Forward Secrecy, VP-63  
 performance  
   improving, AA-370  
   monitoring on Windows NT platforms, AA-405  
 performance guidelines, AA-370  
 Performance Monitor, AA-380  
 period of vulnerability, AA-366  
   description of, AA-319  
 PERMIT/Gate  
   setup, WI-55, OL-50  
 person, AM-34, AM-35  
 ping, AA-398  
   allowing unrestricted, AA-355  
 PIX Address Translation  
   managing, AA-199  
 PIX authentication, WI-59, OL-52  
 PIX blackbox  
   authentication properties, WI-56  
   encryption properties, WI-57  
   location of management server, WI-59, OL-52  
   management guidelines, WI-59, OL-52  
 PointCast, AA-391  
 Policy, see Security Policy  
 pop2, AA-391  
 pop3, AA-391  
 PopUp Alert Command, WI-147, OL-113  
 port 161  
   failure to bind to, AA-241  
 port 256, AA-234  
 port number, WI-84  
   assigning In Address Translation Hide mode, AA-159  
 ports  
   limiting access to specific ports, AA-355  
 Ports Range  
   defining, AA-178  
 postmaster parameter  
   smtp.conf, AA-111  
 Power Management  
   possible conflict with SecurRemote, VP-94  
 PFP, AA-365  
 pre-processor directives, AA-316  
 pre-processor statements, AA-316  
 pre-shared secret, AA-151  
 printing  
   log entries, WI-239, OL-172  
   printing a log  
     truncated fields, AA-340  
 privilege level, AA-225  
 product.conf file, AA-271  
 products.conf file, AA-379  
 prog number, WI-87, OL-70  
 program number, WI-87  
 prologue, WI-89, OL-72  
 prologue, adding to rules, WI-89, OL-72, OL-73  
 prompt\_for\_destination  
   User Authentication, AA-43  
 properties  
   interaction with Rule Base, WI-177  
   network object, WI-15, WI-93, WI-94, OL-23, OL-28, OL-75, OL-83, OL-103  
   of defined object, displaying, WI-82, OL-64  
   of network interface, WI-24, OL-33, OL-40  
   of service object, defining, WI-81, OL-63  
   time object, WI-135  
 Properties button  
   displaying Control Properties windows using, OL-21  
 Properties Setup  
   settings for SecurRemote Client, VP-92  
 Properties Setup windows, WI-141  
 protocol, AA-179  
   which available on network?, AA-353  
 Protocol Selection Criteria window, WI-233  
 Protocol Selection dialog box, OL-162  
 Protocol Selection window, WI-233  
 Protocol Type, OL-67  
 protocol type, WI-84  
 proxy  
   putting behind FireWall-1 HTTP Authenticating Server, AA-45  
 Public Key  
   certifying, VP-5

## LEGEND

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLook GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Master Index      Index-xix



Public Key Distribution System, VP-2  
Public Key Infrastructure, VP-45

## R

RADIUS, AA-30, AA-395, AM-48  
  defining server, WI-99  
  enabling connections from FireWall Module to  
  server, WI-143, OL-109  
  Server Properties window, OL-79  
RADIUS Servers  
  Server Groups, WI-107  
radius\_versions, WI-100, OL-79  
random  
  load balancing algorithm, AA-237  
range of addresses, WI-61  
RAS, AA-391, AA-395  
RDP, AA-395  
reading, further, GS-26  
RealAudio, AA-322, AA-391  
  enabling back connections, AA-391  
  using with SecuRemote Client, VP-92  
re-configuration  
  files modified during, AA-343, AA-345  
reconfiguration options, AA-255  
reconfiguring FireWall-1, AA-254, AA-255  
redirect, AA-398  
refresh, AA-303  
Refresh Network Database utility, OL-171  
refreshing  
  modified IP addresses, OL-171  
Registry  
  FireWall-1 entries, AA-401  
Reject  
  differences from Drop, WI-168, OL-125  
remote sites  
  Account Units, AM-5  
Reply Timeout, WI-143, OL-110  
resend\_period parameter  
  smtp.conf, AA-111  
reserved port, OL-70  
Resolve Address option, OL-165  
resource  
  deleting, OL-85  
resource  
  group, defining properties of, WI-132

## resources

  and synchronized FireWalls, AA-233  
  defining properties of, OL-83

## restrictions

  data not encrypted, VP-93  
  modifying the network configuration after installing  
  SecuRemote, VP-94  
  power management, VP-94  
  removing and adding FireWall adapter, VP-93  
  TCP stacks supported by SecuRemote, VP-93  
  timeout, VP-93  
  user password, VP-93

reverse DNS, WI-118, OL-91

REXEC, OL-112

rexec, AA-391

RFC 1155, AA-241

RFC 1155 - 1213, AA-241

RFC 1156, AA-241

RFC 1157, AA-241

RFC 1521, WI-127, OL-97

RFC 1558, AM-33

RFC 1631, AA-171

RFC 1631 compliant Address Translation  
  feature, AA-156

RFC 1825, VP-8, VP-9

RFC 1826, VP-9

RFC 1827, VP-8

RFC 1828, VP-9

RFC 1829, VP-8

RFC 1852, VP-9

RFC 1858, WI-43, OL-43

RFC 1918, AA-170

RIP, WI-144, OL-110

rip, AA-395

RIP, enabling, WI-144, WI-148, OL-110, OL-115

RLOGIN

  User Authentication, GS-18, AA-29

rlogin, AA-391

Rock Ridge format, GS-57, AA-244, AM-10

round robin

  load balancing algorithm, AA-237

round trip

  load balancing algorithm, AA-237

Route Recording, WI-43

## LEGEND

AA	Architecture and Administration	AM	Account Management Client	GS	Getting Started with FireWall-1
OL	Managing FireWall-1 Using the OpenLook GUI	VP	Virtual Private Networking with FireWall-1	WI	Managing FireWall-1 Using the Windows GUI

Index-xx    FireWall-1 User Guide Master Index • September 1998

Router Access Lists  
   importing, WI-197  
   managing imported access lists, WI-198  
   verifying and viewing, WI-199  
 router interface  
   specifying name of, WI-38  
 router\_load.exe file, AA-377  
 routers  
   anti-spoofing capabilities, WI-39, OL-40  
   anti-spoofing on, WI-38, OL-39  
   auto scoping, WI-38, OL-39  
   defining network object as, OL-33  
   defining properties of, OL-38, OL-48  
   definition of, GS-74  
   installing access lists on, WI-200, OL-142  
   installing Security Policy on, WI-170, WI-194, OL-137  
   uninstalling access lists on, OL-142  
 Routing and Remote Access Service, see Microsoft RRAS  
 Routing Information Protocol, enabling, WI-144, WI-148, OL-110, OL-115  
 routing problems, VP-143  
 RPC  
   enable FireWall-1 to control, WI-146, OL-112  
   securing, GS-17  
   service properties, WI-86, OL-70  
 RPC Control, AA-321  
 RPC Services  
   restriction on use with SecuRemote, VP-92  
 RRAS  
   see Microsoft RRAS  
 RSA, VP-104  
 RSH, OL-112  
   back connections, encrypting, VP-71  
 rsh, AA-391  
 RSH/REXEC, AA-321  
 rshell  
   and Address Translation, AA-171  
 rshell back connections  
   encrypting, VP-71  
 rstat, AA-397  
 Rule Base  
   adding a new rule, AA-180, WI-160, OL-128  
   converting files for Client-Server configuration, AA-280  
   deleting rule from, AA-188, WI-172, OL-129  
   display, WI-158, OL-124  
   generating Inspection Script from, AA-278  
   generating Inspection Script from, using command-line interface, AA-278  
   interaction with Control Properties, OL-132  
   interaction with Properties, WI-177  
   masking rules, WI-178  
   number of rules supported, AA-354  
   sequential application of rules, exception to, AA-104  
   using ping in, AA-355  
   verifying, WI-173, OL-131  
 Rule Base editor tabs, WI-158  
 Rule Base Editor window, OL-21  
 rule zero  
   in Log Viewer, meaning of, AA-352, WI-218, OL-156  
 rulebases.fws file, AA-379  
 rules  
   adding and inserting, WI-160  
   adding to Rule Base, AA-180, WI-160, OL-128  
   consistency and redundancy check of, WI-173, OL-131  
   copying to clipboard, WI-161  
   cutting to clipboard, WI-161  
   default, GS-91  
   deleting, WI-160  
   deleting from Rule Base, AA-188, WI-172, OL-129  
   direction of enforcement, GS-93, GS-96, OL-108  
   disabling, WI-193  
   hiding, WI-178  
   how executed, WI-157, OL-124  
   masking, WI-178  
   modifying, WI-161, OL-130  
   modifying data field values, OL-130  
   pasting from clipboard, WI-161  
   rules, see also Security Policy  
 rundir parameter  
   smtp.conf, AA-111  
 rwall, AA-397

## LEGEND

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLook GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Master Index

Index-xxi

**S**

- S/Key, AA-30, VP-121, AM-48
  - authentication specified in control.map file, AA-348
  - fwal authentication, AA-252
  - Secret Key minimum length, WI-68, WI-69, OL-60, AM-49
  - when a user forgets the password, AA-360
- SA
  - expiration in the course of an encrypted session, VP-38
- saving
  - log entries, WI-239, OL-172
  - log file, WI-239, OL-172
- scan\_period parameter
  - smtp.conf, AA-111
- schema checking, AM-46
- Secret Key
  - sharing, VP-2
- Secure Socket Layer, AA-366
- Secure Socket Layer, see SSL
- SecuRemote
  - and synchronized FireWalls, AA-234
  - configuration example, VP-74, VP-86
  - encapsulated session, VP-94
  - implementation, VP-73
  - other FireWalls along path from Client, VP-91
  - other FireWalls along the path, VP-91
  - restrictions, VP-91
- SecuRemote Client
  - and other firewalls along the path to the SecuRemote Server, VP-91
  - responding to unauthenticated topology requests from, VP-36
- SecuRemote connection
  - reauthenticating, AA-151
- SecuRemote connections
  - encapsulating, VP-55
- SecuRemote daemon
  - description of, VP-104
- SecuRemote kernel module
  - description of, VP-103
- SecuRemote user
  - defining more than one encryption scheme for, VP-78, VP-81
  - defining properties of, VP-77
- SecurID, AA-30, AA-274, AA-391, AA-395, VP-121, AM-48
- securigprop, AA-391
- Security Policy
  - and ISDN interfaces, AA-366
  - backing up, AA-344
  - compiling, AA-257
  - creating new, WI-159
  - default, GS-66, AA-319, AA-320, AA-380
  - downloading to Cisco router, AA-273
  - fetching from Master, AA-259
  - installing, WI-193
  - installing on hosts, OL-148
  - loading, AA-257
  - modified, when implemented, AA-369
  - opening, WI-159
  - preventing two GUI Clients from simultaneously modifying, AA-383
  - removing from selected hosts, OL-148
  - retrieving one installed on FireWall, WI-159
  - uninstalling, AA-259
  - viewing an installed Security Policy, WI-159
- Security Policy, see Rule Base
- Security Servers
  - configuration file, AA-123
  - FTP resource matching, AA-108
  - incoming connections, AA-107
  - interaction with OPSEC products, AA-120
  - outgoing connections, AA-107
  - sending signal to, AA-278
  - using to authenticate other services, AA-125
- Select menu, WI-224
- Selection, WI-237
- selection criteria for Log Viewer, WI-225, OL-157
- selection criteria list, OL-164
- Selection Criteria Manager, WI-225, OL-157, OL-166
- Selection Criteria window, WI-225
- sendmail.exe file, AA-377
- server
  - logical, WI-61
- server load
  - load balancing algorithm, AA-236
- server object

**LEGEND**

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLock GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Index-xxii FireWall-1 User Guide Master Index • September 1998

adding a server to a group, WI-108  
 creating, WI-95  
 creating groups of server objects, WI-107, OL-81  
 defining, WI-93, WI-94  
 deleting, WI-96  
 deleting a server from a group, WI-109  
 modifying, WI-96  
 SERVER\_TIMEOUT, WI-6  
 serverkeys file, AA-378  
 servers  
   logical, OL-25  
 ServerTimeout, WI-6  
 service  
   restoring access to, blocked, AA-336  
   which available on network?, AA-353  
 service object  
   creating new, WI-82  
   defining, WI-81, OL-63  
   deleting, WI-83, OL-65  
   modifying, WI-83  
 Service Properties window, WI-91, OL-65  
 service properties, generic, OL-73  
 service properties, RPC, OL-70  
 service properties, UDP, OL-68  
 Service Selection Criteria window, WI-235  
 services  
   dependence on other services, AA-354  
   which have more than one type, AA-353  
 Services Manager, WI-82, OL-64  
   displaying, WI-8  
 Services Manager window, OL-20  
 Session Authentication  
   configuring, AA-67  
   overview, AA-66  
 Session Authentication Agent  
   required for Session Authentication, AA-29  
 Session Authentication agent  
   configuring, AA-69  
   pre-configuring, AA-70  
 session hijacking, AA-363  
   preventing, AA-363  
 Session Key, VP-24  
 setup.C file, AA-381, WI-100, OL-79  
 Show, WI-238  
 Show All, AM-25  
 Show Null Matches option, OL-164  
 shutdown command, GS-68  
 Single Sign On System Extension, AA-98  
 Single SignOn  
   SecuRemote, VP-125  
 size limit, AM-31  
 SKIP  
   clock synchronization, VP-132  
   rekey policy mismatch, WI-148, OL-114, VP-39  
   restrictions on using with High Availability, AA-233  
   specifying the encrypting gateway's IP  
     address, WI-21, OL-31, VP-25  
 SKIP key  
   changing, OL-121, VP-38  
 slapd.conf  
   modifying, AM-25  
 slapd.conf file, AA-379  
 slapd.pid file, AA-384  
 SLIP, AA-365  
 SMTP  
   badly formed header, WI-123, OL-95  
   pipe, WI-123, OL-95  
   source routing, WI-124, OL-95  
 SMTP resource  
   CVP inspection, WI-127  
   restricting message size, WI-127, OL-97  
 SMTP Security Server, AA-109, AA-361  
   configuration file, AA-111  
   supported protocols, AA-110  
 smtp service, AA-392  
 smtp.conf file, AA-379, WI-124, OL-98  
 smtp.conf.org file, AA-379  
 smtp\_rfc822 property, WI-123, OL-95  
 SNMP, WI-46, OL-45  
   FireWall-1 daemon, GS-11  
   FireWall-1 MIB, AA-382  
   trap, AA-284  
 snmp, AA-395  
 SNMP daemon  
   FireWall-1, AA-241  
   FireWall-1 MIB, AA-382  
   initial keys, AA-242  
   initial communities, AA-242

## LEGEND

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLook GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Master Index      Index-xxiii

optional, AA-241  
 read and write communities (keys), AA-242  
 snmp file, AA-381  
 snmp service, AA-395  
 SNMP Trap Alert Command, WI-147  
 SNMP Trap Alert command, WI-147, OL-113  
 SNMP traps, AA-242  
 snmp.C file, AA-242, AA-379  
 snmp.def file, AA-381  
 snmp\_trap, AA-284  
 snmp\_trap file, AA-377  
 snmpd file, AA-377  
 snmp-trap, AA-395  
 SOFTWARE\CheckPoint\FireWall-1 GUI, WI-6  
 sounds like operator, AM-33  
 Source Object Selection Criteria window, WI-228  
 source port range, WI-84, WI-86, OL-66, OL-68  
 source-quench, AA-398  
 Specific Sign-on, AA-82  
 SPI  
   defining, VP-66  
   using, VP-65  
 spoof tracking, GS-99  
 spoofing, GS-99, AA-338, WI-25, OL-35  
 SQLNet, AA-392  
 sqlnet2, AA-322  
   and Address Translation, AA-171  
 Src Routing, WI-43  
 SrcSpoofing (3Com), WI-43  
 SSL, AA-366, AM-1, AM-3, AM-25  
   default, AM-18  
   negotiating parameters for, AM-20  
   port number for LDAP connection, WI-106  
 SSL connections, WI-106  
 SSL fingerprint  
   confirming with the LDAP Server's system  
     administrator, AM-20  
 Standard Sign-on, AA-82  
 Standard.W file, AA-379  
 starts with operator, AM-33  
 state directory, AA-384  
 state tables  
   cleared when Security Policy re-installed, AA-345  
 Static Destination mode, AA-164  
 Static Source mode, AA-162  
 status  
   of FireWalled hosts, displaying, AA-264  
   of hosts, displaying using command-line  
     interface, AA-264  
 status display  
   updating and changing, WI-204, OL-147  
 status\_alert, AA-284  
 status\_alert file, AA-377  
 std.def file, AA-381  
 stderr  
   rsh/rexec reverse stderr connections, AA-391,  
     WI-146  
 stdin  
   message describing alert available in, OL-114  
 Steelhead, see Microsoft RRAS  
 StreamWorks, AA-395  
 suggested reading, GS-26  
 SunNetManager, AA-382  
 suspected intruders  
   blocking connections to and from, WI-215  
 switch  
   defining network object as, OL-33  
   definition of, GS-74  
   setup, WI-49  
   Xylan, WI-49, OL-48, OL-49  
 Sybase SQL, AA-392  
 synch, AA-303  
 synchronization  
   timing issues, AA-232  
 synchronized FireWall Modules  
   restrictions on implementation, AA-232  
 synchronized FireWalls  
   resources, AA-233  
   restrictions, AA-232  
 synchronizing FireWall Modules  
   on different platforms, AA-232  
 SYNDefender, OL-116  
   guidelines for choosing between methods, AA-333  
   when changes to Maximum Sessions take  
     effect, WI-150  
 SYNDefender Gateway  
   description of, AA-331  
 SYNDefender.Passive Gateway  
   description of, AA-333

## LEGEND

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLook GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Index-xxiv    FireWall-1 User Guide Master Index • September 1998



syntax differences  
     NT and Unix, AA-253  
 syslog, AA-395, WI-45, OL-44  
 syslogd, WI-45, OL-44  
 System Status  
     displaying, WI-8  
 system status  
     changing and updating display of, WI-204, OL-147  
     monitoring, GS-128  
 System Status View window, GS-128  
 System Status window, GS-11, WI-202, OL-146

**T**

table.def file, AA-381  
 tables  
     synchronizing, AA-303  
 TACACS, AA-30, AA-273, AA-395, AM-48  
 TACACS authentication connection, AA-274  
 TACACS Server  
     enabling connections from FireWall Module to, WI-143, OL-109  
 TACACS servers  
     defining, WI-100  
 TACACS+, AA-392  
 Talk protocol, AA-365  
 TCP  
     service properties, WI-83  
 TCP connections  
     established, AA-322  
 TCP sequence number prediction, AA-363  
 TCP Session Timeout, WI-143, OL-109  
 TCP sessions  
     established, AA-322  
 TCP Stacks  
     supported by SecuRemote, VP-93  
 tcpip.def file, AA-381  
 TELNET  
     FireWall-1 daemon, AA-356  
     User Authentication, GS-18, AA-29  
 telnet, AA-392  
 TELNET daemon, AA-356  
 template  
     changing, AM-58  
     creating, AM-57  
     deleting, AM-58  
     effect of modifications to on attached users, AM-58  
     user, OL-57  
 tftp, AA-395  
 time object  
     creating, WI-136  
     creating groups of time objects, WI-139, OL-106  
     defining, WI-135, OL-103  
     deleting, WI-136  
     editing existing, WI-136  
     groups, WI-139  
     modifying, WI-136  
     properties, WI-135  
 time object group  
     deleting from, WI-140  
 time service, AA-392, AA-396  
 Time Stamping, WI-43  
 time-exceeded, AA-398  
 timeout, OL-69, OL-71  
     caused by delay of entering user name and password, VP-93  
     connection to Management Server, WI-6  
 timeout parameter  
     smtp.conf, AA-111  
 timestamp, AA-383, AA-398  
 timestamp reply, AA-398  
 timestamp request, AA-398  
 TimeStep, WI-55  
     setup, WI-55  
 TimeStep Integrated FireWall  
     setup, WI-55  
 timing issues  
     synchronization, AA-232  
 Tiny Fragments, WI-43  
 tmp directory, AA-384  
 tod, AA-309  
 topology download, VP-83, VP-112  
 traceroute, AA-396  
 transitional links option, GS-56  
 Transparent Authentication, AA-28  
 trap  
     SNMP, AA-284  
 TRAP macro, AA-316  
 trapexec.conf file, AA-379

**LEGEND**

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLook GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Master Index

Index-xxv

traps.def file, AA-381  
 traps.h file, AA-381  
 tree object  
   creating in LDAP directory, AM-24  
 troubleshooting  
   installation, VP-142  
   no SecuRemote Server along route, VP-143  
   routing, VP-143  
 truncated fields  
   when printing a log, AA-340  
 tty warning, AA-341  
 two or more FireWalls  
   going across for authenticated services, AA-359  
 Type Selection Criteria window, WI-230

## U

UDP  
   enabling replies, WI-143, OL-110  
   service properties, WI-85, OL-68  
 UDP Replies, OL-110  
 UDP response, WI-45, OL-44  
 UFP Server  
   step by step procedure for using, AA-131  
 UFP server, OL-77  
 UFP Servers, WI-96, OL-77  
 UFP servers  
   defining, WI-96  
 uninstalling  
   router access list, OL-142  
   uninstalling a Security Policy, AA-259  
   uninstalling SecuRemote, VP-108  
   uninstalling the Account Management Client, AM-13  
 Unix and NT syntax differences, AA-253  
 Unix platforms  
   minimum requirements, GS-55  
 Unknown Network Objects, WI-199, OL-140  
 upgrading  
   FireWall-1 loses its state after, GS-35  
   objects carried over from previous version, GS-34  
   reinstalling Security Policy after, AA-345  
   to the current version from earlier versions, GS-34  
   what objects are carried over from previous  
   version, AA-344  
 URI Specification File  
   format, WI-121, OL-94

URL Filtering, AA-130  
 URL filtering  
   step by step procedure, AA-130  
 user  
   changing the template to which a user is  
   attached, AM-44  
   defining new, AM-44  
   deleting, AM-45  
   generic, AA-325, WI-72, OL-61  
   group, defining properties of, WI-73  
   modifying, AM-44  
   restricting internal user's access to JAVA  
   applets, WI-123  
 User Authentication  
   authentication rule, WI-175, OL-134  
   defining on a per-user rather than a per-group  
   basis, AA-357  
   deployment, AA-32  
   description of, GS-98  
   GUI interface, AA-41  
   overview, AA-31  
   tracking and timeout parameters, AA-36  
 User Authentication Alert Command, WI-147,  
 OL-114  
 User Database  
   downloading, AA-264, WI-64, WI-79, OL-56  
   exporting, AA-285  
   importing, AA-285  
   installing, see User Database, downloading  
   when changes take effect, WI-78, OL-61, OL-138  
 User Defined Alert Command, WI-147, OL-113  
 user group  
   adding to source of rule, WI-162  
   in rule, WI-162  
   restricting access based on, WI-162  
 User Password  
   restrictions, VP-93  
 user properties, WI-66, OL-58  
 user.def file, AA-381  
 userc.c file  
   installing standard version of, VP-82, VP-83,  
   VP-106, VP-111  
 User-Defined Service Properties  
   Example, WI-89, OL-74  
 users

## Legend

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLock GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Index-xxvi FireWall-1 User Guide Master Index • September 1998



defining in both LDAP and FireWall-1, AA-142,  
 AA-154  
 exporting from FireWall-1 database to LDAP  
 directory, AA-152  
 restricting internal user's access to JAVA  
 applets, WI-123, OL-87  
 Users Manager  
 displaying, WI-8  
 Users Manager window, OL-20  
 Uses H.323, AA-390  
 utilities, OL-143  
 utilities, additional, OL-149  
 uuwp, AA-392

## V

Valid Addresses, WI-25  
 value of data field  
 modifying, OL-130  
 VDO-Live, AA-392  
 enabling back connections, AA-392  
 VDOLive, AA-322, AA-325, WI-85, OL-67  
 using with SecuRemote Client, VP-92  
 version  
 specifying the FireWall-1 version, WI-23  
 version 3.0 and earlier  
 compatibility with Version 4.0, GS-34  
 version 4.0  
 compatibility with earlier versions, GS-34  
 version number  
 displaying, AA-267  
 View menu, WI-178  
 viewing  
 Inspection Script, WI-194, OL-137  
 log, WI-211, OL-151  
 VIRSIG.DAT file, AA-377  
 Virtual Encryption Session, VP-23  
 virtual interfaces, AA-363  
 Virtual Link encryption features, WI-59, OL-52  
 virtual packet reassembly, AA-363  
 Vosaic, AA-392  
 VPN-1 Module, GS-81  
 VPN-1 Secure Center  
 configuration, AM-4  
 VPN-1 SecuRemote/n, GS-81

## W

WAIS, OL-68  
 wals, AA-392  
 WebTheatre, AA-322, AA-393  
 Wellfleet  
 managing Access Lists, AA-280  
 Wellfleet See Bay Networks  
 Wellfleet, see Bay Networks  
 wellfleet.C file, AA-381, AA-385  
 wellfleet.mib file, AA-382, AA-385  
 who service, AA-396  
 Width window, WI-220  
 Windows NT  
 monitoring performance, AA-405  
 Windows Registry, AA-372  
 FireWall-1 entries, AA-401  
 WinFrame, AA-393  
 workstation objects  
 listing in hosts and lmhosts files, WI-22, WI-36,  
 OL-28, OL-38  
 www.opsec.com, AA-120

## X

X.25, AA-365  
 X/Motif  
 obtaining a license for, GS-69  
 starting the GUI, GS-88, WI-4  
 starting the Log Viewer, WI-212  
 starting the System Status View, WI-202  
 where to install license, GS-69  
 X/Motif libraries  
 version used by FireWall-1, GS-59, GS-68  
 X11, AA-393  
 Xing, AA-395  
 and Address Translation, AA-171  
 xlate.conf file, AA-379  
 Xlated Destination Port Selection Criteria  
 window, WI-230  
 Xlated Dst Selection Criteria window, WI-229  
 Xlated Source Port Selection Criteria window, WI-230  
 Xlated Src Selection Criteria window, WI-229  
 xtreme.def file, AA-381  
 XView  
 limitation on number of menu objects, OL-32

## LEGEND

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLook GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Master Index

Index-xxvii

Xylan, GS-74, GS-77, GS-97  
installing Encryption Module on, GS-77  
Xylan switch  
defining network object as, OL-33  
setup, WI-49, OL-48, OL-49

#### Y

ypbind, AA-397  
yppasswd, AA-397  
ypserv, AA-397  
ypupdated, AA-397  
ypxfrd, AA-397

#### LEGEND

AA Architecture and Administration	AM Account Management Client	GS Getting Started with FireWall-1
OL Managing FireWall-1 Using the OpenLook GUI	VP Virtual Private Networking with FireWall-1	WI Managing FireWall-1 Using the Windows GUI

Index-xxviii FireWall-1 User Guide Master Index • September 1998